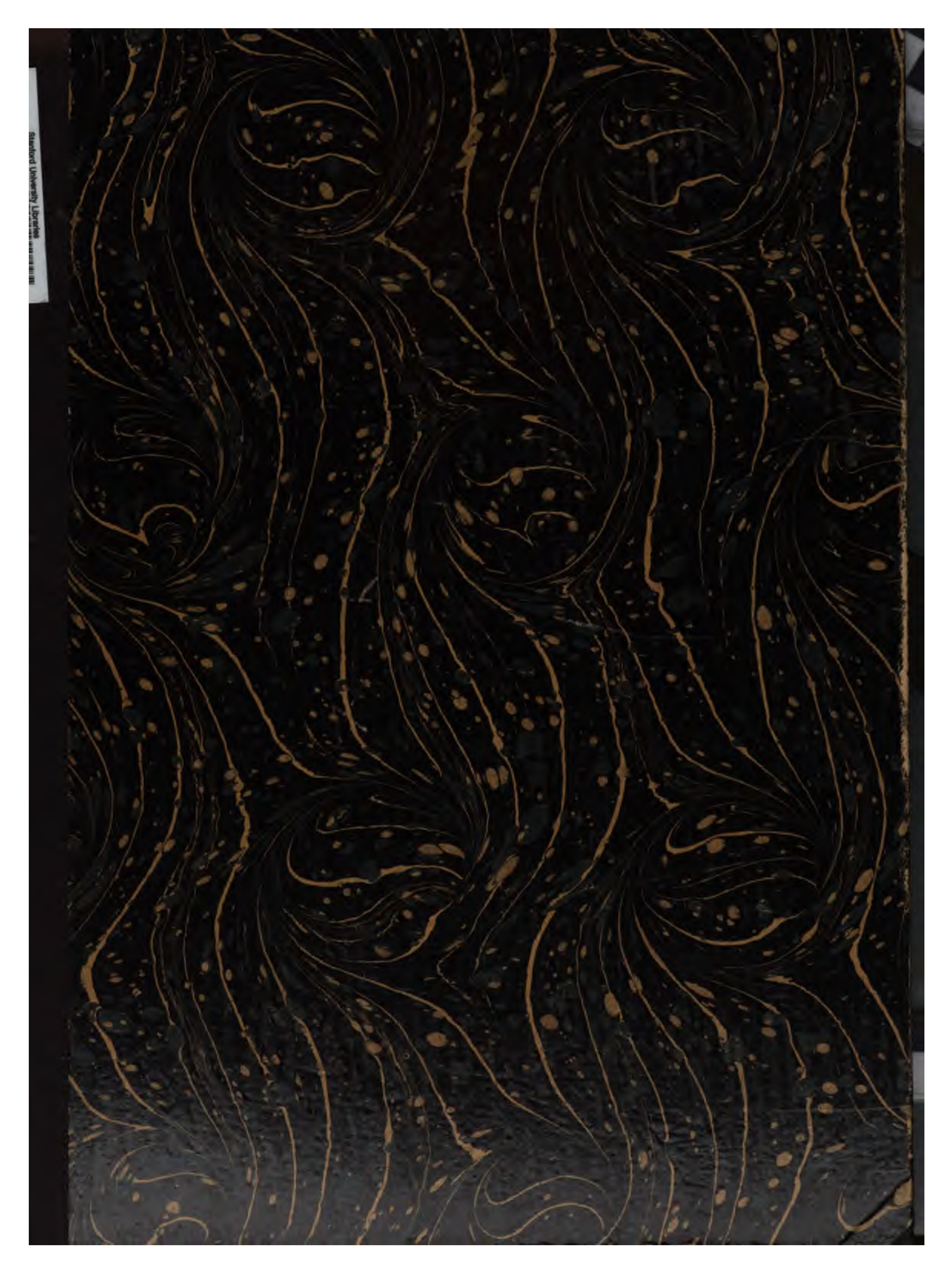


Stanford University Libraries

Journal

für die

reine und angewandte Mathematik.

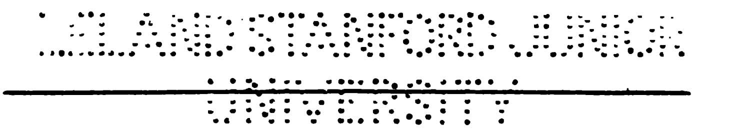
In zwanglosen Heften.

Herausgegeben

von

A. L. Crelle.

Mit thätiger Beförderung hoher Königlich-Preufsischer Behörden.



Acht und zwanzigster Band.

In vier Heften.

Mit sieben lithographirten Tafeln.

Berlin, 1844.

Bei G. Reimer.

Et se trouve à Paris chez Mr. Bachelier (successeur de Mme Ve Courcier),
Libraire pour les Mathématiques etc. Quai des Augustins No. 55.

Inhaltsverzeichnifs
des acht und zwanzigsten Bandes, nach den Gegenständen.

I. Reine Mathematik.

Nr. der Abhandlung.

1. Analysis.

Heft. Seite.

2. Geometrie.

II. Angewandte Mathematik.

Aufgaben.

1.

Über die Zusammensetzung gerader Linien und eine daraus entspringende neue Begründungsweise des barycentrischen Calculs.

(Von Herrn Professor *A. F. Möbius* zu Leipzig.)

---

1. **D**ie einzigen Sätze der Geometrie, die ich hierbei als erwiesen voraussetze, sind die zwei: „dafs zwei Gerade, deren jede mit einer dritten parallel ist, auch mit einander parallel sind," und „dafs Parallelen zwischen Parallelen einander gleich sind."

Im Folgenden soll durch Setzung des Gleichheitzeichens zwischen die Ausdrücke zweier geraden Linien, z. B. durch $AB = CD$, stets angezeigt werden, dafs die zwei Linien nicht blofs von gleicher Länge sind, sondern auch einerlei Richtung haben, so dafs, wenn die eine Linie CD parallel mit sich fortgeführt wird, bis C mit A zusammenfällt, dann auch D mit B coïncidirt. Mit dieser Bezeichnungsart lassen sich jene zwei Sätze kurz also ausdrücken:

I. Ist $AB = CD$ und $CD = EF$, so ist auch $AB = EF$.

II. Ist $AB = CD$, so ist auch $AC = BD$.

Hieraus läfst sich sogleich weiter schliefsen:

III. Ist 1) $AB = A'B'$ und 2) $BC = B'C'$, so ist auch $AC = A'C'$.

Denn nach II. folgt aus 1): $AA' = BB'$, und aus 2): $BB' = CC'$; folglich nach I.: $AA' = CC'$; folglich nach II.: $AC = A'C'$.

IV. Ist 1) $AB = A'B'$, 2) $BC = B'C'$, 3) $CD = C'D'$, 4) $DE = D'E'$, etc., so ist auch $AD = A'D'$, $AE = A'E'$, etc. Denn aus 1) und 2) folgt nach III.: $AC = A'C'$; hieraus und aus 3) eben so: $AD = A'D'$; etc.

2. Sind AB, CD, EF mehrere, ihrer Gröfse und Richtung nach gegebene gerade Linien, und setzt man, von einem beliebigen Puncte P ausgehend, diese Linien parallel mit ihren Richtungen aneinander, macht also $PQ = AB$, $QR = CD$, $RS = EF$ und bildet somit die gebrochene Linie $PQRS$, so soll diese Operation die *Zusammensetzung* oder die *geometrische Addition* der gegebenen Linien heifsen; zum Unterschiede von der

arithmetischen, als wobei blofs die Gröfse der Linien, nicht auch ihre Richtung in Betracht kommt. Die gerade Linie vom Anfangspuncte P bis zum Endpuncte S der gebrochenen Linie $PQRS$ nenne man die *geometrische Summe* der Linien AB, ... und drücke dieses hier aus durch

$$AB + CD + EF = PS.$$

Fällt der Endpunct S mit dem Anfangspuncte P zusammen, so ist die geometrische Summe Null, und man schreibe alsdann

$$AB + CD + EF = 0.$$

Wenn AB, CD und EF dieselbe Summe wie GH und IK haben, so schreibe man, um dieses auszudrücken:

$$AB + CD + EF = GH + IK.$$

Übrigens ist von selbst klar, dafs, wie auch die Puncte $A, B, C, D, \ldots$ im Raume liegen mögen, stets sein wird:

$$AB + BA = 0, \qquad AB + BC = AC,$$
$$AB + BC + CA = 0, \quad AB + BC + CD = AD, \quad \text{u. s. w.}$$

3. Wenn man, um AB, ... zusammenzusetzen, statt P irgend einen andern Punct P' zum Ausgangspuncte wählt und hiernach $P'Q' = AB$, $Q'R' = CD$, $R'S' = EF$ macht, so ist nach I.: $PQ = P'Q'$, $QR = Q'R'$, $RS = R'S'$, und daher nach IV.: $PS = P'S'$; d. h. die geometrische Summe bleibt dieselbe, welches auch der Punct sei, von welchem man bei der Addition ausgeht.

Die geometrische Summe mehrerer Linien ist aber nicht blofs von dem Orte des Ausgangspunctes, sondern auch von der Ordnung, in welcher man sie zusammensetzt, unabhängig. Denn macht man, um AB und CD zu addiren, das einemal, mit AB anfangend, $PQ = AB$, $QR = CD$, und das andremal, mit CD anfangend, $PQ' = CD$, $Q'R' = AB$, so ist hiernach 1) $PQ = Q'R'$ und 2) $PQ' = QR$; folglich wegen 1): $PQ' = QR'$, und $= QR$ wegen 2); also R' mit R identisch, so dafs sich das eine- wie das andremal PR als Summe ergiebt. Eben so können überhaupt bei mehrern zu addirenden Linien irgend zwei nächstfolgende mit einander vertauscht werden; und da man von irgend einer Aufeinanderfolge mehrerer Elemente durch fortgesetztes Vertauschen je zweier nächstfolgenden zu jeder andern Folge der Elemente gelangen kann, so wird auch bei mehrern geometrisch zu addirenden Linien, ganz wie bei der arithmetischen Addition, die Ordnung, in welcher man sie nach und nach verbindet, jede beliebige sein können.

4. Sind die Linien AB, CD, EF, GH, IK ihrer Gröfse und Richtung nach gegeben, und macht man, von P ausgehend, $PQ=AB$, $QR=CD$, $RS=EF$, $ST=GH$, $TU=IK$, so ist $AB+CD+EF=PS$, $GH+IK=SU$ und $AB+CD+\ldots+IK=PU$, $=PS+SU$, nach 2. zu Ende. Setzt man daher

$$(a.)\quad AB+CD+EF=LM \quad \text{und} \quad (b.)\quad GH+IK=NO,$$

so ist $LM=PS$, $NO=SU$ und $AB+CD+\ldots+IK=PS+SU=LM+NO$; d. h. man kann die Formeln ($a.$) und ($b.$), und eben so drei und mehrere solcher Formeln zu einander addiren.

Ist die zu ($a.$) zu addirende Formel mit ($a.$) identisch, so kommt:

$$AB+CD+EF+AB+CD+EF = LM+LM,$$

oder, wenn man, da Linien in jeder beliebigen Ordnung addirt werden können (3.), je zwei gleichnamige unmittelbar auf einander folgen läfst, und unter $m.AB$ eine Linie versteht, welche mit AB einerlei Richtung und eine Länge hat, die sich zu der von AB wie m zu 1 verhält:

$$2.AB+2.CD+2.EF = 2.LM,$$

und eben so, wenn man m, mit ($a.$) identische Formeln addirt:

$$(c.)\quad m.AB+m.CD+m.EF = m.LM;$$

wo m jede ganze positive Zahl sein kann.

Unter derselben Voraussetzung in Betreff von m kann man aus ($a.$) schliefsen, dafs

$$\frac{1}{m}.AB+\frac{1}{m}.CD+\frac{1}{m}.EF = \frac{1}{m}.LM.$$

Denn setzt man $\frac{1}{m}.AB+\frac{1}{m}.CD+\frac{1}{m}.EF=XY$, so ist auch, weil man mit m multipliciren kann: $AB+CD+EF=m.XY$; folglich wegen ($a.$): $m.XY=LM$, und daher $XY=\frac{1}{m}.LM$.

Eine Formel, wie ($a.$), kann man daher, ohne ihre Richtigkeit aufzuheben, mit jeder ganzen positiven Zahl, folglich auch mit jedem rationalen positiven Bruche, also, nach bekannten Schlüssen, auch mit jeder irrationalen positiven Zahl multipliciren oder dividiren *).

---

*) Dasselbe läfst sich auch leicht mit Hülfe der Lehre von ähnlichen Figuren darthun; so wie umgekehrt diese Lehre aus obigem Satze abgeleitet werden kann. So folgt z. B. aus der identischen Gleichung $AB+BC=AC$, dafs auch $m.AB+m.BC=m.AC$ ist. Setzt man daher $m.AB=FG$ und $m.BC=GH$, so wird $m.AC=FG+GH=FH$; d. h., sind zwei Seiten FG, GH eines Dreiecks den Seiten AB, BC eines andern parallel und ihnen proportional, so ist auch die dritte Seite FH des erstern der dritten Seite AC

Das für die Formel (a.) jetzt Bewiesene mufs endlich auch für Formeln von der allgemeinen Form

$$(a^*.) \qquad a.AB + c.CD + \ldots\ldots = l.LM$$

gelten, wo a, c, ... und l beliebige positive Zahlen bedeuten. Denn wenn man darin $a.AB = A'B'$, $c.CD = C'D'$, etc. und $l.LM = L'M'$ setzt, so wird diese Form auf die vorige (a.) zurückgeführt.

5. So wie in der Arithmetik $a + b = c$ und $a = c - b$ identische Gleichungen sind, so kann man auch hier die Formeln

$$1. \quad AB + CD = EF \quad \text{und} \quad 2. \quad AB = EF - CD$$

als identisch betrachten und AB den *geometrischen Unterschied* zwischen EF und CD nennen, wenn EF die geometrische Summe von AB und CD ist. Setzt man zu (1.) auf beiden Seiten DC hinzu, so kommt: $AB = EF + DC$, $= EF - CD$ nach (2.); wonach eine Linie von einer andern geometrisch *subtrahiren* nichts anderes heifst, als dieselbe Linie, nach der entgegengesetzten Richtung genommen, zu der andern geometrisch *addiren*.

Wenn daher in der obigen allgemeinen Formel (a.), gegen die dortige Annahme, eines oder etliche Glieder negative Zeichen haben, so kann man, verlangt man blofs positive Glieder, entweder das Minuszeichen eines Gliedes geradezu in Plus verwandeln, mufs aber dann noch den Anfangs- und den Endpunct der zugehörigen Linie mit einander vertauschen: oder man kann das negative Glied blofs mit Änderung seines Vorzeichens auf die andere Seite des Gleichheitszeichens setzen.

Überhaupt geht aus dem Bisherigen hervor, dafs man dergleichen Formeln, wie (a.), vollkommen so wie gewöhnliche Gleichungen behandeln kann, dafern sie nur rücksichtlich der in ihnen vorkommenden Linien stets von linearer Form bleiben, so dafs man nämlich Glieder von der einen Seite des Gleichheitszeichens auf die andere mit dem entgegengesetzten Vorzeichen bringen, alle Glieder mit derselben Zahl multipliciren oder dividiren, und zwei oder

---

des letztern parallel und ihr in demselben Verhältnisse proportional. Oder sind FG, GH, HF resp. den AB, BC, CA parallel, und setzt man deshalb $FG = p.AB$, $GH = q.BC$, $HF = r.CA$, so kommt durch Addition dieser Formeln: $0 = p.AB + q.BC + r.CA$. Immer ist aber auch $r.AB + r.BC + r.CA = 0$, und daher (Nr. 5.) $(p-r)AB + (q-r)BC = 0$. So lange aber A, B, C nicht in einer Geraden liegen, kann von zwei Linien, welche die Richtungen AB und BC haben, die geometrische Summe nicht Null sein, und es mufs dann folglich jeder der Coëfficienten $p - r$ und $q - r$ einzeln Null sein, also $p = q = r$ und $FG : GH : HF = AB : BC : CA$; d. h. wenn die Seiten eines Dreiecks FGH denen eines andern ABC parallel sind, so sind sie ihnen auch proportional.

mehrere solcher Formeln zu einander addiren, oder die eine von der andern subtrahiren kann.

6. Wir sind somit zu einer Rechnungsart mit geraden Linien gelangt, deren Richtigkeit, so lange die Linien Theile einer und derselben Geraden, oder mit derselben Geraden parallel sind, keines Beweises bedarf, und deren Zuläfslichkeit, wenn die Linien verschiedene Richtungen haben, aus den allerersten Sätzen der Parallelentheorie fliefst.

Es läfst sich aber diese Rechnung mit Linien noch auf eine eigenthümliche Weise umgestalten; und dieses in Folge einer merkwürdigen Beziehung, welche bei geometrisch zu addirenden Linien zwischen den Anfangs- und Endpuncten der Linien Statt findet. Man habe z. B. die Linien AB und CD zu addiren. Da immer $AB = AD + DB$ und $CD = CB + BD$ ist, so wird $AB + CD = AD + DB + CB + BD = AD + CB$, indem $DB + BD = 0$ ist. Sind demnach A, B, C, D irgend vier Puncte im Raume, so erhält man dasselbe Resultat, man mag die Linien AB und CD, oder die Linien AD und CB zusammensetzen; mit andern Worten: *zur Zusammensetzung zweier Linien reicht es schon hin, dafs man weifs, welches ihre Anfangspuncte* (A und C) *und welches ihre Endpuncte* (B und D) *sind, nicht aber wie letztere zur erstern gehören* (ob B zu A und D zu C, oder D zu A und B zu C).

Dasselbe Princip gilt nun, wie man leicht sieht, auch bei der Zusammensetzung von drei und mehreren Linien. Denn sollen z. B. die drei Linien AB, CD und EF addirt werden, so kann man zuerst, weil die Ordnung, in welcher sie addirt werden, willkürlich ist, und man daher beliebige zwei zu den zwei ersten nehmen kann, irgend zwei Endpuncte, wie B und D, oder D und F, oder B und F, mit einander vertauschen. Können aber von mehrern in gewisser Ordnung auf einander folgenden Elementen je zwei mit einander vertauscht werden, so lassen sie sich durch Wiederholung dieser Operation in jede beliebige Ordnung bringen, und man kann folglich die Endpuncte B, D, F auf jede beliebige Weise mit den Anfangspuncten A, C, E verbinden, so dafs z. B.

$$AB + CD + EF = AF + CB + ED.$$

Eben so läfst sich statt $AB + BC + CA$, worin A, B, C die Anfangspuncte und B, C, A die Endpuncte sind, setzen: $AA + BB + CC$; und da jede der Linien AA, BB, CC offenbar für sich Null ist, so mufs auch $AB + BC + CA = 0$ sein (vergl. No. 2.).

7. Da es also bei jeder beliebigen Anzahl geometrisch zu addirender Linien immer nur darauf ankommt, zu wissen, welches die Anfangspuncte und welches die Endpuncte sind, nicht aber wie letztere mit erstern zusammengehören, so wollen wir alle diese Puncte isolirt schreiben und zur Unterscheidung den Anfangspuncten das positive, den Endpuncten das negative Zeichen geben, wollen also statt $AB+CD+EF$

$$A-B+C-D+E-F, \quad \text{oder} \quad A+C+E-B-D-F$$

schreiben; oder wie man sonst diese sechs Buchstaben mit ihren Zeichen auf einander folgen lassen will. Auch wird diese Ausdrucksweise noch dadurch gerechtfertigt, daſs, so wie der Ausdruck AA, geometrisch genommen, eine Linie $=0$ bezeichnet, auch $A-A$ in arithmetischem Sinne $=0$ ist. In Übereinstimmung mit der Natur der geometrischen Zusammensetzung läſst sich daher die von einem Puncte zu einem andern zu ziehende gerade Linie, als durch welche der Unterschied zwischen der Lage der beiden Puncte bestimmt wird, im Calcul durch den Unterschied der beiden Puncte selbst ausdrücken.

Da ferner, eben so wie $AB+CD=AD+BC$, auch $a.AB+a.CD = a.AD+a.BC$ ist, so wird man auch, wenn in einer Formel Glieder mit numerischen Coëfficienten, wie $a.AB$, etc. vorkommen, statt derselben, $aA-aB$, etc., und daher statt

$$(a.) \quad a.AB+c.CD+\ldots. = l.LM \text{ schreiben können:}$$
$$(a.^*) \quad aA-aB+cC-cD+\ldots. = lL-lM;$$

und jede Folgerung, welche man aus $(a.)$ allein, oder aus $(a.)$ in Verbindung mit noch andern ihr ähnlichen Formeln, nach den in Nr. 5. bemerkten Regeln ziehen kann, ist dieselbe; und keine anderen wird man auch aus $(a.^*)$ und den ihr ähnlichen Formeln ableiten können. Liegen z. B. vier Puncte A, B, C, D so, daſs $AB+2CD=2BC$, so wird man statt dessen $A-B+2C-2D = 2B-2C$ oder $A+4C=3B+2D$ schreiben und daraus unter Andern folgern können: $4C-4B+B-A=2D-2A$, d. i. $4CB+BA=2DA$.

Mit Formeln, wie $(a.^*)$, wird es demnach gestattet sein, alle die arithmetischen Operationen vorzunehmen, bei welchen sie in Bezug auf die in ihnen enthaltenen Puncte von linearer Form bleiben; wobei noch der Vortheil Statt findet, daſs man sich der Formeln, welche in geometrischer Bedeutung identisch sind, wie $AB+BC=AC$, nicht mehr zu erinnern braucht, indem solche in arithmetisch-identische $(A-B+B-C=A-C)$ übergehen.

8. Soll umgekehrt eine Formel, deren Glieder Producte aus Zahlen in Puncte sind, Sinn und Bedeutung haben, so muſs die Summe aller Zahlen

auf der einen Seite des Gleichheitszeichens der Summe der Zahlen auf der andern Seite gleich sein, d. h. die Formel mufs auch dann noch richtig sein, wenn alle Puncte weggestrichen werden.

So wird z. B. zum Bestehen der Formel

$$1. \quad aA+bB = cC$$

erfordert, dafs $a+b=c$ ist. In der That wird alsdann

$$aA-aC = bC-bB, \quad \text{d. i.} \quad a.AC = b.CB.$$

Haben aber, wie hierdurch angezeigt wird, die Linien AC und CB einerlei Richtung, und überdies den Punct C gemein, so liegt C mit A und B in einer Geraden. Die Formel (1.) drückt daher aus, dafs A, B und C in einer Geraden liegen, und dafs sich dabei $AC:CB = b:a$ verhält.

Damit die Formel

$$2. \quad aA+bB+cC = dD$$

bestehe, mufs $a+b+c=d$ sein; woraus

$$aA-aD+bB-bD = cD-cC,$$

$$\text{d. i.} \quad a.AD+b.BD = c.DC$$

folgt. Da die aus $a.AD$ und $b.BD$ zusammengesetzte Linie offenbar in der durch AD und BD zu legenden Ebene enthalten, oder doch mit der Ebene ABD parallel sein mufs, und die Linie die Richtung DC haben, also durch den Punct D der Ebene gehen soll, so wird durch (2.) ausgedrückt, dafs A, B, C und D in einer Ebene liegen.

Dasselbe folgt auch daraus, dafs, wenn man

$$(\alpha.) \quad aA+bB = (a+b)E \quad \text{und daher}$$

$$(\beta.) \quad (a+b)E+cC = (a+b+c)D$$

setzt, E mit A und B, und D mit E und C in einer Geraden liegt, also AB und CD sich in einem Puncte E schneiden. Dabei verhält sich

$$(\gamma.) \quad AE:EB = b:a \quad \text{und} \quad ED:DC = c:a+b.$$

Mit diesen Proportionen läfst sich, wenn die Puncte A, B, C und die Verhältnisse zwischen a, b, c gegeben sind, der Punct D bestimmen. Die linke Seite der Gleichung (2.) wird hiernach der *Ausdruck* des auf der rechten Seite stehenden Punctes D genannt. Eben so ist in (1.) $aA+bB$ der *Ausdruck* von C. Umgekehrt hat jeder mit A und B in einer Geraden liegende Punct einen Ausdruck von der Form (1.), und jeder mit A, B und C in einer Ebene liegende Punct einen Ausdruck von der Form (2.).

In dem besondern Falle, wenn in (2.) $a+b=0$, also $b=-a$ ist, mufs $d=c$ sein. Aus (2.) wird alsdann: $aA-aB = cD-cC$, also

$a.AB = c.DC$, d. h. die Linien AB und DC sind einander parallel und verhalten sich wie c und a. Zu demselben Resultate gelangt man auch durch die Proportion (γ.), welche, wenn $b = -a$ ist, $AE:BE = 1:1$ giebt. Dieses ist aber, so lange A und B zwei verschiedene Puncte sein sollen, nicht anders möglich, als wenn E, oder der Durchschnitt von CD mit AB, unendlich entfernt liegt. Bemerken wir daher noch, dafs $aA - aB$ oder $A - B$, als Ausdruck eines Punctes genommen, einen in der Richtung AB unendlich entfernten Punct ausdrückt.

In dem Falle, wenn in der Gleichung (2.) die Summe $a+b+c=0$ ist, wird D, zufolge (β.), ein unendlich entfernter Punct in der Geraden EC, also ein in der Ebene ABC nach einer bestimmten Richtung unendlich weit liegender Punct.

Ähnlicherweise zeigt sich, dafs, wenn A, B, C, D nicht in einer Ebene liegen und

$$3. \quad aA + bB + cC + dD = (a+b+c+d)E$$

gesetzt wird, E ein durch die Lage von A, B, C, D und durch die Verhältnisse zwischen a, b, c, d unzweideutig bestimmter Punct im Raume ist; dafs, wenn $a+b+c+d=0$ ist, E unendlich entfernt nach einer bestimmten Richtung liegt, und dafs umgekehrt jeder Punct im Raume durch einen Ausdruck von der Form (3.) dargestellt werden kann.

9. Die Rechnung mit Formeln der Art, wie (1.), (2.), (3.), ist es nun, die ich in meiner Schrift vom Jahre 1827 die „barycentrische" genannt habe. Offenbar ist die gegenwärtige Herleitung dieser Formeln einfacher, als die in jener Schrift gegebene, indem dort ihre Erklärung noch ein System fremdartiger Hülfslinien erforderte. Es wurde nämlich die Formel

$$(\alpha.) \quad aA + bB + cC + \ldots = (a+b+c+\ldots)S$$

als der abgekürzte Ausdruck der Gleichung

$$(\beta.) \quad a.AA' + b.BB' + c.CC' + \ldots = (a+b+c+\ldots)SS'$$

angesehen, wo A', B', C', ... und S' die Durchschnitte einer beliebig gelegten Ebene ε mit Linien waren, die man durch A, B, C, ... und S, parallel mit einer willkürlichen die ε schneidenden Richtung l gelegt hatte *).

*) Die Gleichung (β.) kann aus der Formel (α.) auch sehr leicht mittelst der hier zum Grunde gelegten Principien hergeleitet werden. Es ist nämlich die Formel (α.) gleichbedeutend mit

$$a.AS + b.BS + c.CS + \ldots = 0,$$

oder, da $AS = AA' + A'S' + S'S$, etc. ist, gleichbedeutend mit

$$a(AA' + A'S' + S'S) + b(BB' + B'S' + S'S) + \ldots = 0,$$

Von der andern Seite kann freilich nicht geleugnet werden, dafs bei einer solchen Erklärung jedes Glied der Formel eine mathematische Bedeutung erhält, während bei der hier gegebenen Darstellung die einzelnen Glieder nicht als wirkliche Gröfsen, sondern nur, ich möchte sagen, durch ein Spiel des Calculs zum Vorschein kommen. Wie dem aber auch sein mag, so dürfte doch das hier über die geometrische Addition Gesagte, und der innige Zusammenhang, in welchem diese Lehre mit der barycentrischen Rechnung steht, einer Mittheilung nicht ganz unwerth gewesen sein.

---

oder mit $TU+VW=0$, wenn man

$$a(AA'+S'S)+b(BB'+S'S)+\ldots = TU \text{ und}$$
$$a.A'S'+b.B'S'+\ldots = VW$$

setzt. Da aber AA', BB', ... und SS' sämmtlich mit der Linie l parallel sind, und $A'S'$, $B'S'$, ... in der Ebene ε liegen, so mufs auch TU mit l und VW mit ε parallel sein; VW kann daher nicht mit l oder TU parallel sein, weil l und ε sich schneiden sollen. Mithin kann die geometrische Summe von TU und VW nicht anders Null sein, als wenn jede dieser Linien einzeln Null ist. Dies giebt die Formeln

$$a(AA'+S'S)+b(BB'+S'S)+\ldots = 0 \text{ und}$$
$$a.A'S'+b.B'S'+\ldots = 0,$$

von denen die erstere einerlei mit der zu beweisenden (β.) ist, die letztere aber anzeigt, dafs, wenn die geometrische Summe mehrerer Linien Null ist, auch die geometrische Summe der Projectionen dieser Linien auf eine beliebige Ebene durch Parallelen mit einer beliebigen Geraden Null ist.

2.

Angenäherte Bestimmung der Function $\Gamma(1+n) = \int_0^\infty x^n e^{-x}\,dx$, wenn n eine ganze, gebrochene, oder incommensurable sehr grofse positive Zahl ist.

(Von Herrn Professor *Raabe* in Zürich.)

Zweite Abhandlung.

Im 25sten Bande dieses Journals habe ich die Grenzwerthe der in der Überschrift angedeuteten Function für den Fall angegeben, wenn n irgend eine positive, jedoch nur ganze Zahl vorstellt. So z. B. habe ich in No. 7. dieser Abhandlung unter mehreren andern Ergebnissen auch folgende zwei Ungleichheiten aufgestellt:

$$\Gamma(1+n) > n^n \sqrt{(2n\pi)}e^{-n}, \quad \Gamma(1+n) < n^n \sqrt{(2n\pi)}e^{-n}e^{\frac{1}{n}Y_1},$$

wo

$$Y_1 = \frac{1}{2\pi^2}\left(1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots\right) = \frac{1}{12}$$

ist, deren Begründung mir daselbst jedoch nur für positive *ganze* Werthe gelang. Nun hätte ich allerdings der von einigen Analysten beliebten Schlufsweise mich gleichfalls bedienen können, nämlich: „Da die Ausdrücke zur „Linken und Rechten der Ungleichheitszeichen dieser hier aufgestellten Un„gleichheiten continuirliche Functionen für sämmtliche positive Werthe von n „verbleiben, so bestehen solche nicht nur für alle positiven ganzen Werthe von n, „wie bewiesen wurde, sondern auch für gebrochene und incommensurable „Werthe dieser Gröfse," um die allgemeine Gültigkeit dieser Ungleichheiten zu erhärten; allein wie unhaltbar eine solche Schlufsweise bei genauer Erwägung derselben sei, wird Jeder beistimmen, der mit Aufmerksamkeit in der Functionenlehre sich umgesehen und nur das, wovon er ungetrübte Einsicht erlangt, auszusagen gewohnt ist. Mit der gegenwärtigen zweiten Abhandlung

beabsichtige ich nun, die oben erwähnte Beschränkung der in der ersten Abhandlung gewonnenen Ergebnisse, dafs solche nämlich nur für positive ganze Werthe von n bestehen, auf eine durchaus einleuchtende Weise zu beseitigen; wozu ich sofort übergehe.

1.

Wir beginnen unsere Untersuchungen, indem wir, eben wie in der ersten Abhandlung, das die Function $\Gamma(x)$ betreffende allgemeinste Theorem zu Grunde legen.

Dieses Theorem stellt die Gleichheit

$$\Gamma(na) = \Gamma(a)\Gamma\left(a+\frac{1}{n}\right)\Gamma\left(a+\frac{2}{n}\right)\dots\Gamma\left(a+\frac{n-1}{n}\right)n^{na-\frac{1}{2}}(2\pi)^{\frac{1}{2}(1-n)}$$

auf, die für sämmtliche positiven Werthe von a, und nur für positive ganze Werthe von n, Bestand hat.

Läfst man in dieser Gleichheit n eine unendlich grofswerdende Zahl sein, so gelangt man, wie in No. 2. der ersten Abhandlung, auf die Gleichheit

$$\int_a^{a+1}\log\Gamma(x)\,dx = \omega\log\Gamma\left(\frac{a}{\omega}\right)+(a-\tfrac{1}{2}\omega)\log\omega+\tfrac{1}{2}(1-\omega)\log 2\pi,$$

wo ω eine unendlich-klein werdende, a eine beliebige reelle, jedoch nicht negative Gröfse vorstellt. Diese Gleichheit kann man auch wie folgt stellen:

$$(\alpha.)\quad \int_a^{a+1}\log\Gamma(x)\,dx = \tfrac{1}{2}\log 2\pi+f(a),$$

wenn abkürzend

$$(\beta.)\quad f(a) = \omega\log\Gamma\left(\frac{a}{\omega}\right)+a\log\omega$$

gesetzt wird.

Die Function $f(a)$, wie solche durch die Gleichung $(\beta.)$ dargestellt wird, erscheint wegen der unendlich-klein werdenden Gröfse ω unter unbestimmter Form; dieselbe nun von dieser Gröfse ω zu befreien, so wie dann auch den Werth des bestimmten Integrals in $(\alpha.)$ bei jeder nicht negativen reellen Verfügung über a dargestellt zu erhalten, verfahren wir wie folgt.

1) Fassen wir zuerst den Fall ins Auge, wenn a eine unendlich-klein werdende positive Gröfse vorstellt, von der Form $m\omega$, wo m irgend eine endliche und positive Zahl bedeutet.

Unter dieser Annahme geht die Gleichung $(\beta.)$ in

$$f(m\omega) = \omega\log\Gamma(m)+m\omega\log\omega,$$

über, aus welcher

$$f(0) = 0$$

gezogen wird; folglich hat man nach (α.) die Integralbestimmung

$$1.\quad \int_0^1 \log \Gamma(x)\,dx = \tfrac{1}{2}\log 2\pi,$$

welche mit der aus der Gleichung (3.) der ersten Abhandlung einerlei ist.

2) Wenn a eine reelle positive ganze Zahl vorstellt, so gelangt man zur Kenntnifs von $f(a)$ nach directer Bestimmung des Integrals in (α.) auf folgendem Wege.

Nach einer bekannten Relation der Function $\Gamma(x)$ hat man, wenn a eine ganze Zahl ist,

$$\Gamma(x+a) = x(x+1)(x+2)\ldots.(x+a-1)\,\Gamma(x).$$

Wird diese Gleichung logarithmisch aufgelöset, dann mit dx multiplicirt und von $x=0$ bis $x=1$ integrirt, so erhält man, mit Zuziehung der vorhin aufgestellten Integralbestimmung in (1.), die Gleichung

$$\int_0^1 \log \Gamma(x+a)\,dx$$

$$= \int_0^1 \log x\,dx + \int_0^1 \log(x+1)\,dx + \ldots. \int_0^1 \log(x+a-1)\,dx + \tfrac{1}{2}\log 2\pi.$$

Man hat aber, wenn r eine von x unabhängige Gröfse vorstellt, die Integralgleichung

$$\int_0^1 \log(x+r)\,dx = (1+r)\{\log(1+r)-1\} - r\{\log r - 1\},$$

aus welcher, eben wie in der ersten Abhandlung, die folgende gezogen wird:

$$\int_0^1 \log \Gamma(x+a)\,dx = \sum_{r=1}^{r=a}\{r\log r - 1\} - \sum_{r=1}^{r=a-1}\{r\log r - 1\} + \tfrac{1}{2}\log 2\pi,$$

die mit folgender gleichbedeutend ist:

$$2.\quad \int_0^1 \log \Gamma(x+a)\,dx = a(\log a - 1) + \tfrac{1}{2}\log 2\pi.$$

Wird hier in dem bestimmten Integrale linkerhand die Integrationsvariable x durch $x-a$ ersetzt, so ergiebt sich endlich folgende Integralbestimmung:

$$3.\quad \int_a^{a+1} \log \Gamma(x)\,dx = \tfrac{1}{2}\log 2\pi + (\log a - 1),$$

welche, eben wie die vorhergehende (die mit der Gleichung (4.) der ersten Abhandlung einerlei ist), für alle positiven ganzen Werthe von a, den Nullwerth mitbegriffen, abgeleitet und sonach, vorläufig wenigstens, blofs für diese Werthe als bestehend anzusehen ist.

Vergleicht man ferner diese Gleichung (3.) mit der oben aufgestellten Gleichung (α.), so ergiebt sich, da $\log \Gamma(x)$, wenn nur die reellen Werthe



ins Auge gefafst werden, als eine eindeutige Function von x zu erkennen ist, folgende Bestimmungsgleichung für $f(a)$:

$$4.\quad f(a) = a(\log a - 1),$$

die, eben wie die vorhergehende (3.), als nur für positive ganze Werthe von a, mitbegriffen den Nullwerth, bestehend vorläufig anzusehen ist. Dafs die hier gewonnenen drei Gleichungen (2.), (3.) und (4.) für alle reellen und nicht negativen Werthe von a Bestand haben, werden wir in folgendem dritten Fall darthun.

3) Wenn nämlich, drittens, a eine nicht ganze, jedoch positive Zahlengröfse vorstellt, so begründen wir die Richtigkeit der eben ausgesprochenen Behauptung in folgender Weise. In der Gleichung (β.) ist man für a jede nicht negative reelle Zahl zu setzen berechtigt. Wird nun in derselben $a = \frac{p}{q}$ gesetzt, wo p und q beliebige positive ganze Zahlen vorstellen, die keinen ganzen Factor gemein haben, so geht sie in folgende über:

$$f\left(\frac{p}{q}\right) = \omega \log \Gamma\left(\frac{p}{q\omega}\right) + \frac{p}{q} \log \omega,$$

oder auch in

$$qf\left(\frac{p}{q}\right) = q\omega \log \Gamma\left(\frac{p}{q\omega}\right) + p \log \omega.$$

Da nun q nur eine endliche, wenn auch noch so grofse Zahl vorstellen darf, so wird $q\omega$ eine unendlich-klein werdende Zahl sein, die durch ω' dargestellt und, in letzte Gleichung eingeführt, dieselbe in folgende verwandelt.

$$qf\left(\frac{p}{q}\right) = \omega' \log \Gamma\left(\frac{p}{\omega'}\right) + p \log \omega' - p \log q.$$

Die Gleichung (β.) bietet aber vermöge der Unbestimmtheit jeder unendlich-klein werdenden Gröfse die folgende dar:

$$f(p) = \omega' \log \Gamma\left(\frac{p}{\omega'}\right) + p \log \omega';$$

also giebt die Subtraction dieser von der vorhergehenden Gleichung folgende:

$$qf\left(\frac{p}{q}\right) - f(p) = -p \log q.$$

Bedenkt man endlich, dafs man nach der oben aufgestellten Gleichung (4.), da p eine ganze positive Zahl vorstellt, die Gleichung

$$f(p) = p(\log p - 1)$$

hat, so giebt die vorhergehende Gleichung folgende:

$$qf\left(\frac{p}{q}\right) = p(\log p - 1) - p \log q,$$

die mit

$$f\left(\frac{p}{q}\right) = \frac{p}{q}\left(\log\frac{p}{q} - 1\right)$$

einerlei ist, und aus welcher das Bestandhaben der Gleichung (4.) für rationale gebrochene positive Werthe von a auf unzweideutige Weise hervorgeht.

Was endlich die irrationalen oder incommensurabeln Werthe von a betrifft, so folgt das Bestandhaben der Gleichung (4.) für dergleichen Werthe von a aus dem Umstande, dafs so ein Werth von a jedesmal zwischen zwei rationale gebrochene Zahlenwerthe gedacht werden kann, deren Unterschied jede beliebige Kleinheit eingehen kann; und da für jeden der letzteren zwei Werthe von a die Gleichung (4.), wie oben bewiesen wurde, Bestand hat, so besteht solche vermöge der Continuität des Ausdruckes rechterhand dieser Gleichung auch für sämmtliche Zwischenwerthe, und sonach auch für die erstgenannten Werthe von a; w. z. b. w.

Es besteht also, dieses vorausgesetzt, die oben aufgestellte Gleichung (2.), die in unserer ersten Abhandlung nur für positive ganze Werthe von a nachgewiesen war, wie auch die aus derselben gefolgerte Gleichung (3.), für alle positiven reellen Werthe von a.

2.

Nunmehr wenden wir uns der im Eingange der vorhergehenden Nr. aufgestellten allgemeinen Relation der Function $\Gamma(x)$ abermals zu. Multiplicirt man solche mit na und berücksichtigt die Gleichheit

$$\Gamma(1+z) = z\Gamma(z),$$

so geht sie in folgende über:

$$\Gamma(1+na)$$
$$= \Gamma(a)\Gamma\left(a+\frac{1}{n}\right)\Gamma\left(a+\frac{2}{n}\right)\dots\Gamma\left(a+\frac{n-1}{n}\right)(na)^{na+\frac{1}{2}}a^{-na+\frac{1}{2}}(2\pi)^{\frac{1}{2}(1-n)},$$

die für alle positiven reellen Werthe von a Bestand hat. Wird diese nun logarithmisch aufgelöset und hierauf durch n dividirt, so hat man

$$\frac{1}{n}\log\frac{\Gamma(1+na)}{(na)^{na}\sqrt{(2na\pi)}}$$
$$= \frac{1}{n}\left\{\log\Gamma(a)+\log\Gamma\left(a+\frac{1}{n}\right)+\log\Gamma\left(a+\frac{2}{n}\right)+\dots+\Gamma\left(a+\frac{n-1}{n}\right)\right\}$$
$$-\left(a-\frac{1}{2n}\right)\log a - \frac{1}{2}\log 2\pi,$$

oder auch folgende Gleichung:

$$\frac{1}{n}\log\frac{\Gamma(1+na)}{(na)^{na}\sqrt{(2na\pi)}}$$
$$=\frac{1}{n}\left\{\tfrac{1}{2}\log\Gamma(a)+\log\Gamma\left(a+\frac{1}{n}\right)+\ldots+\log\Gamma\left(a+\frac{n-1}{n}\right)+\tfrac{1}{2}\log\Gamma(a+1)\right\}$$
$$-a\log a-\tfrac{1}{2}\log 2\pi.$$

Wird hier $na=\alpha$ gesetzt, so wird α vermöge der Willkürlichkeit der positiven reellen Zahl a jede positive reelle Zahl vorstellen können. Dadurch geht dann diese Gleichheit über in:

$$\frac{1}{\alpha}\log\frac{\Gamma(1+\alpha)}{\alpha^{\alpha}\sqrt{(2\alpha\pi)}}$$
$$=\frac{1}{\alpha}\left\{\tfrac{1}{2}\log\Gamma(a)+\log\Gamma\left(a+\frac{a}{\alpha}\right)+\log\Gamma\left(a+\frac{2a}{\alpha}\right)+\ldots+\log\Gamma\left(a+\frac{(n-1)a}{\alpha}\right)\right.$$
$$\left.+\tfrac{1}{2}\log\Gamma(a+1)\right\}-\log a-\frac{1}{2a}\log 2\pi,$$

oder auch, wenn einstweilen

$$\nu=\frac{a}{\alpha}=\frac{1}{n}$$

gesetzt wird, in folgende:

$$\frac{a}{\alpha}\log\frac{\Gamma(1+\alpha)}{\alpha^{\alpha}\sqrt{(2\alpha\pi)}}$$
$$=\nu\{\tfrac{1}{2}\log\Gamma(a)+\log\Gamma(a+\nu)+\log\Gamma(a+2\nu)+\ldots+\log\Gamma(a+(n-1)\nu)$$
$$+\tfrac{1}{2}\log\Gamma(a+1)\}-a\log a-\tfrac{1}{2}\log 2\pi,$$

wo a und α beliebige positive reelle Zahlengrößen sind, die wegen $an=\alpha$ der einzigen Beschränkung, den Quotienten $\frac{\alpha}{a}$ als ganze Zahl darzustellen, unterliegen. Die weitere Umformung dieser Gleichheit, namentlich die Verbindung derselben mit der in vorhergehender Nr. unter (2.) aufgestellten Gleichheit, werden wir in der folgenden Nr. mittheilen.

3.

Wir legen dasselbe Theorem zum Grunde, von dem wir in der ersten Abhandlung, in Nr. 4., Gebrauch machten, und verweisen zum bessern Verständnisse des nun Folgenden auf diese so eben citirte Nr.

Setzen wir der Kürze wegen

$$\log\Gamma(a+x)=\varphi(x)$$

und bezeichnen die aufeinander folgenden Differentialquotienten von $\varphi(x)$ durch $\varphi_1(x)$, $\varphi_2(x)$, ... $\varphi_{2m}(x)$, so haben wir gemäfs diesem Theoreme für den gegenwärtig beabsichtigten Zweck vorerst festzustellen, dafs der $2m$te Differentialquotient von $\varphi(x)$, nämlich $\varphi_{2m}(x)$, für alle Werthe von $x=0$ bis $x=1$

einerlei Vorzeichen habe. Dieses findet sich, ähnlich wie in der ersten Abhandlung, folgendermaßsen.

Nach dem Begriffe der Function $\Gamma(x)$ hat man die Gleichung

$$\varphi(x) = (x+a-1)\log k + \log 1.2.3.4\ldots k - \sum_{r=0}^{r=k-1} \log(a+r+x),$$

wo das Summenzeichen über alle ganzen Zahlenwerthe von $r=0$ bis $r=k-1$ sich erstreckt und k eine unendlich-grofs werdende positive Zahl ist. Stellt man nun die successiven Differentialquotienten von $\varphi(x)$ her, so ergeben sich folgende Bestimmungsgleichungen:

$$\varphi_1(x) = \log k - \sum_{r=0}^{r=k-1} \frac{1}{a+r+x},$$

$$\varphi_2(x) = \sum_{r=0}^{r=k-1} \frac{1}{(a+r+x)^2},$$

$$\varphi_3(x) = -1.2 \sum_{r=0}^{r=k-1} \frac{1}{(a+r+x)^3},$$

$$\varphi_4(x) = \quad 1.2.3 \sum_{r=0}^{r=k-1} \frac{1}{(a+r+x)^4},$$

. . . .

$$\varphi_{2m-1}(x) = -1.2.3\ldots.(2m-2) \sum_{r=0}^{r=k-1} \frac{1}{(a+r+x)^{2m-1}},$$

$$\varphi_{2m}(x) = +1.2.3\ldots.(2m-1) \sum_{r=0}^{r=k-1} \frac{1}{(a+r+x)^{2m}}.$$

Die letzte dieser Gleichungen zeigt augenfällig, dafs die Function $\varphi_{2m}(x)$ für sämmtliche reellen Werthe von x, und sonach auch, wie oben verlangt wurde, für alle Werthe von $x=0$ bis $x=1$ ein und dasselbe Vorzeichen, und zwar das positive annimmt.

Da ferner aus diesen eben aufgestellten Gleichungen die folgenden sich ergeben:

$$\varphi_1(1)-\varphi_1(0) = \frac{1}{a},$$

$$\varphi_3(1)-\varphi_3(0) = \frac{1.2}{a^3},$$

$$\varphi_5(1)-\varphi_5(0) = \frac{1.2.3.4}{a^5},$$

. . . .

$$\varphi_{2m-1}(1)-\varphi_{2m-1}(0) = \frac{1.2.3.4\ldots.(2m-2)}{a^{2m-1}};$$

so giebt das am Eingange erwähnte Theorem, auf den vorliegenden Fall an-

gewandt, folgende Gleichheit in Bezug auf alle positiven Werthe von a:

$$\int_0^1 \log\Gamma(a+x)\,dx$$

$$= \nu\{\tfrac{1}{2}\log\Gamma(a)+\log\Gamma(a+\nu)+\ldots.+\log\Gamma(a+(n-1)\nu)+\tfrac{1}{2}\log\Gamma(a+1)\}$$

$$-\frac{1}{a}Y_2\nu^2+\frac{1.2}{a^3}Y_4\nu^4-\ldots.+(-1)^m\frac{1.2.3.4\ldots.(2m-2)}{a^{2m-1}}Y_{2m}\nu^{2m},$$

wo $n\nu=1$ ist, und Y_2, Y_4, Y_6, ... die in No. 4. der ersten Abhandlung festgestellten Bedeutungen beibehalten.

Durch Vergleichung dieses Ergebnisses mit dem Ausgangs voriger Nr. aufgestellten ergiebt sich folgende Gleichheit:

$$\int_0^1 \log\Gamma(a+x)\,dx$$

$$= a\log a+\tfrac{1}{2}\log 2\pi+\frac{a}{\alpha}\log\frac{\Gamma(1+\alpha)}{\alpha^\alpha\sqrt{(2\alpha\pi)}}$$

$$-\frac{1}{a}Y_2\nu^2+\frac{1.2}{a^3}Y_4\nu^4-\ldots.+(-1)^m\frac{1.2.3.4\ldots.(2m-2)}{a^{2m-1}}Y_{2m}\nu^{2m},$$

wo $\nu=\frac{1}{n}=\frac{a}{\alpha}$ ist. Eliminirt man ν; so geht diese Gleichheit auch in folgende über:

$$\int_0^1 \log\Gamma(a+x)\,dx$$

$$= a\log a+\tfrac{1}{2}\log 2\pi+\frac{a}{\alpha}\log\frac{\Gamma(1+\alpha)}{\alpha^\alpha\sqrt{(2\alpha\pi)}}$$

$$-a\left\{\frac{1}{\alpha^2}Y_2-\frac{1.2}{\alpha^4}Y_4+\ldots.+(-1)^{m-1}\frac{1.2.3.4\ldots.(2m-2)}{\alpha^{2m}}Y_{2m}\right\}.$$

Diese Gleichheit mit der in Nr. 1. unter (2.) aufgestellten verbunden, die für dieselben Werthe von a besteht, giebt nach Weglassung des gemeinsamen Factors a folgende als das Endziel der vorliegenden Abhandlung anzusehende Gleichheit:

$$\log\frac{\Gamma(1+\alpha)}{\alpha^\alpha\sqrt{(2\alpha\pi)}}$$

$$=-\alpha+\frac{1}{\alpha}Y_2-\frac{1.2}{\alpha^3}Y_4+\frac{1.2.3.4}{\alpha^5}Y_6-\ldots.(-1)^{m-1}\frac{1.2.3.4\ldots.(2m-2)}{\alpha^{2m-1}}Y_{2m},$$

die für alle positiven Werthe von α mit einer Genauigkeit besteht, daſs die numerische Gröſse des Unterschiedes beider Theile der Gleichheit kleiner als das Schluſsglied derselben ist.

Die Gleichung (5.) in Nr. unserer ersten Abhandlung stimmt, wenn der Buchstab n daselbst durch α ersetzt wird, mit der so eben aufgestellten Gleichung in allen Stücken überein; nur ist solche bloſs für positive ganze Zahlen-

werthe der allgemeinen Buchstabengröße a daselbst begründet werden. Nachdem wir sie von dieser Beschränkung befreit haben, finden auch alle in Nr. 5., 6. und 7. besagter Abhandlung angestellten Betrachtungen und gewonnenen Ergebnisse, die von jener Beschränkung durchaus unabhängig sind, ihre ungeschmälerte Anwendung; wir verweisen daher auf die oben citirten Nrn. jener Abhandlung, um die Endergebnisse, die wir in folgender Schlußnummer zusammenstellen werden, als begründet angeben zu dürfen.

4.

Zuerst hat man, wenn a irgend eine reelle und positive Zahl vorstellt, mitbegriffen den Nullwerth, die Gleichheit:

$$\Gamma(1+a)=a^a\sqrt{(2a\pi)}e^{-a}.e^{\frac{1}{a}Y_2}.e^{-\frac{1.2}{a^3}Y_4}.e^{-\frac{1.2.3.4}{a^5}Y_6}....e^{(-1)^{m-1}\frac{1.2.3....(2m-2)}{a^{2m-1}}Y_{2m}},$$

wo

$$Y_{2r}=\frac{2}{(2\pi)^{2r}}\left\{1+\frac{1}{2^{2r}}+\frac{1}{3^{2r}}+\frac{1}{4^{2r}}+....\right\}$$

für alle ganzen und positiven Werthe von r ist. Diese Gleichheit giebt das möglichst genaueste Resultat, wenn die ganze und positive Zahl m zwar kleiner als $a\pi$, jedoch nur sehr wenig davon verschieden ist.

Um die Größe der Genauigkeit, mit welcher $\Gamma(1+a)$ nach dieser Gleichheit geschätzt werden kann, besser zu beurtheilen, berücksichtige man folgende Ungleichheiten:

$$\Gamma(1+a)>a^a\sqrt{(2a\pi)}e^{-a},$$

$$\Gamma(1+a)<a^a\sqrt{(2a\pi)}e^{-a}.e^{\frac{1}{a}Y_2},$$

$$\Gamma(1+a)>a^a\sqrt{(2a\pi)}e^{-a}.e^{\frac{1}{a}Y_2}.e^{-\frac{1.2}{a^3}Y_4},$$

$$\Gamma(1+a)<a^a\sqrt{(2a\pi)}e^{-a}e^{\frac{1}{a}Y_2}.e^{\frac{1.2}{a^3}}.e^{\frac{1.2.3.4}{a^5}Y_6},$$

u. s. w.,

die, wie die obige Gleichheit, gleichfalls für sämmtliche positiven reellen Werthe von a, Null mitbegriffen, Bestand haben.

Somit haben wir denn die Ergebnisse der ersten Abhandlung, die wir in Nr. 7. daselbst zusammenstellten, von der dort am Schlusse ausgesprochenen Beschränkung befreit und dadurch das uns am Eingange vorliegender Abhandlung gesteckte Endziel erreicht, so daß der Gegenstand dieser beiden Abhandlungen, für jetzt wenigstens, für geschlossen zu erklären ist.

Zürich, im April 1843.

3.

Reduction des *p*fachen Integral-Ausdrucks

$$\int_0^\infty\int_0^\infty\int_0^\infty \varphi\left(a_1 x_1^{n_1} + a_2 x_2^{n_2} + \ldots + a_p x_p^{n_p}\right) x_1^{r_1-1} x_2^{r_2-1} \ldots x_p^{r_p-1}\, dx_1\, dx_2 \ldots dx_p,$$

in welchem $a_1, a_2, \ldots a_p, n_1, n_2, \ldots n_p, r_1, r_2, \ldots r_p$ constante Gröfsen, $x_1, x_2, \ldots x_p$ die Integrationsvariabeln sind und φ eine beliebige Function ist, auf ein einfaches, dieselbe Function φ enthaltendes bestimmtes Integral.

(Von Herrn Prof. *Raabe* in Zürich.)

Im zweiten Bande meiner Differenzial- und Integralrechnung, in Nr. 322., habe ich das Doppel-Integral

$$\int_0^\infty\int_0^\infty \varphi(x^2+y^2)\, dx\, dy$$

durch Umsetzung der Integrationsvariabeln x und y in u und v mittels der zwei Gleichungen

$$x = v\cos u, \qquad y = v\sin u,$$

von der Ausmittelung eines einfachen bestimmten Integrals abhängig dargestellt und durch die vermittelnden Gleichungen folgende Reductionsgleichung gefunden:

$$\int_0^\infty\int_0^\infty \varphi(x^2+y^2)\, dx\, dy = \tfrac{1}{4}\pi\int_0^\infty \varphi(x)\, dx.$$

Nachdem ich diesen, als den synthetischen Theil der Lösung erreicht, habe ich dann auf analytischem Wege, durch Umsetzung der Variabeln x und y im Doppel-Integrale linkerhand in $x\sqrt{a}$ und $y\sqrt{b}$, folgende allgemeine Reductionsgleichung erhalten:

$$\int_0^\infty\int_0^\infty \varphi(a x^2 + b y^2)\, dx\, dy = \frac{\pi}{4\sqrt{(ab)}}\int_0^\infty \varphi(x)\, dx.$$

Ganz in ähnlicher Weise werde ich mich in der vorliegenden Abhandlung zuerst mit dem synthetischen Theile befassen, der, wie der Erfolg zeigen wird, blofs die Reduction des Doppel-Integrals

$$\int_0^\infty\int_0^\infty \varphi(x^n + y^n)\, dx\, dy$$

auf ein einfaches bestimmtes Integral betrifft, und dann auf analytischem Wege nach und nach zu der in der Überschrift ausgesprochenen Reduction fortgehen.

1.

Das Doppel-Integral

$$\int_0^\infty\int_0^\infty \varphi(x^m+y^n)\,dx\,dy,$$

in welchem φ eine beliebige Function bedeutet und m sowohl als n angebbare positive, reelle Werthe sind, ist durch Einführung zweier neuen Integrationsvariabeln statt der x und y zuletzt auf ein einfaches, die Function φ noch enthaltendes bestimmtes Integral zurückzubringen möglich: wie sofort gezeigt werden soll. Wir stellen zu diesem Zwecke folgende zwei Gleichungen auf:

$$1.\quad x^m = v^2\cos u^2,\qquad y^n = v^2\sin u^2,$$

wo also u und v die neuen Integrationsvariabeln sind, und bestimmen dann die Integrationsgrenzen dieser einzuführenden Integrationsvariabeln, so wie die nach diesen zu integrirende Differenzialfunction, nach der im zweiten Bande meiner Differenzial- und Integralrechnung in Nr. 321. gegebenen Anleitung.

Wird nämlich die neueingeführte Variable v aus den eben aufgestellten zwei Gleichungen eliminirt, so ergiebt sich

$$x^m\sin u^2 - y^n\cos u^2 = 0.$$

Da diese Gleichung bei der eben festgestellten Verfügung über die Exponenten m und n sowohl für jede der beiden Annahmen

$$x = 0 \quad\text{und}\quad x = \infty$$

constante Werthe für u giebt, nämlich:

$$u = \tfrac{1}{2}\pi \quad\text{und}\quad u = 0,$$

als auch für jede der folgenden:

$$y = 0 \quad\text{und}\quad y = \infty,$$

dergleichen Werthe für u, nämlich

$$u = 0 \quad\text{und}\quad u = \infty,$$

so folgt, dass gegenwärtig ohne Unterschied die eine oder die andere der in der eben citirten Nr. aufgestellten Umformungsgleichungen eines Doppel-Integrals, die in (15.) oder die in (21.), zu Grunde gelegt werden darf. Stellt man nun aus den Gleichungen (1.) den Ausdruck für

$$J = \frac{dx}{du}\cdot\frac{dy}{dv} - \frac{dx}{dv}\cdot\frac{dy}{du}$$

her, so ergiebt sich

$$\Delta = -\frac{4}{mn} v^{\frac{2}{m}+\frac{2}{n}-1} \sin u^{\frac{2}{n}-1} \cos u^{\frac{2}{m}-1};$$

wodurch man folgende Umformungsgleichung erhält:

$$\int_0^\infty\int_0^\infty \varphi(x^m+y^n)\,dx\,dy = \frac{4}{mn}\int_0^{\frac{1}{2}\pi}\int_0^\infty \varphi(v^2) v^{\frac{2}{m}+\frac{2}{n}-1} \sin u^{\frac{2}{n}-1} \cos u^{\frac{2}{m}-1}\,dv\,du,$$

die auch mit folgender gleichbedeutend ist:

$$\int_0^\infty\int_0^\infty \varphi(x^m+y^n)\,dx\,dy = \frac{4}{mn}\int_0^{\frac{1}{2}\pi} \sin u^{\frac{2}{n}-1} \cos u^{\frac{2}{m}-1}\,du . \int_0^\infty \varphi(v^2) v^{\frac{2}{m}+\frac{2}{n}-1}\,dv;$$

und da aus dieser die Bestimmung unseres vorgelegten Doppel-Integrals von der eines Products zweier, in keinerlei gegenseitigen Abhängigkeit stehenden einfachen Integrale abhängig erkannt wird, so ist der eigentliche synthetische Theil der Aufgabe jetzt herbeigeführt; von der aus wir nunmehr auf analytischem Wege das im Eingange gesteckte Endziel zu erreichen trachten werden.

Berücksichtiget man zuerst die in Nr. 222. des ersten Bandes unserer Differenzial- und Integralrechnung aufgestellte Gleichung (48.), vermöge welcher

$$\int_0^{\frac{1}{2}\pi} \sin u^{\frac{2}{n}-1} \cos u^{\frac{2}{m}-1}\,du = \frac{1}{2}\,\frac{\Gamma\left(\frac{1}{m}\right).\Gamma\left(\frac{1}{n}\right)}{\Gamma\left(\frac{1}{m}+\frac{1}{n}\right)}$$

ist, wo die Function $\Gamma(z)$ durch die Gleichung

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x}\,dx$$

definirt wird; so geht die obige Umformungs- oder Reductionsgleichung in

$$\int_0^\infty\int_0^\infty \varphi(x^m+y^n)\,dx\,dy = \frac{2}{mn}\cdot\frac{\Gamma\left(\frac{1}{m}\right).\Gamma\left(\frac{1}{n}\right)}{\Gamma\left(\frac{1}{m}+\frac{1}{n}\right)}\int_0^\infty \varphi(v^2) v^{\frac{2}{m}+\frac{2}{n}-1}\,dv,$$

oder auch, mit Beachtung der durch die Gleichheit

$$2.\quad \Gamma(1+z) = z\Gamma(z)$$

ausgedrückten Eigenthümlichkeit der Function $\Gamma(z)$, in

$$(\alpha.)\quad \int_0^\infty\int_0^\infty \varphi(x^m+y)\,dx\,dy = 2\,\frac{\Gamma\left(1+\frac{1}{m}\right).\Gamma\left(1+\frac{1}{n}\right)}{\Gamma\left(\frac{1}{m}+\frac{1}{n}\right)}\int_0^\infty \varphi(v^2) v^{\frac{2}{m}+\frac{2}{n}-1}\,dv$$

über; die für alle positiven angebbaren reellen Werthe von m und n Bestand hat.

2.

Mit Hülfe der in der vorigen Nr. gewonnenen Reductionsgleichung (α.) sind wir auch den dreifachen Integral-Ausdruck

$$\int_0^\infty\int_0^\infty\int_0^\infty \varphi(x^m+y^n+z^p)\,dx\,dy\,dz,$$

in welchem m, n, p reelle und positive angebbare Werthe haben und der nur noch von der Ausmittelung eines einzigen einfachen bestimmten Integrals abhängig ist, welches dieselbe, durchaus willkürliche Function φ enthält, darzustellen im Stande.

Es besteht nämlich, besagter Reductionsgleichung (α.) gemäfs, folgende Gleichung:

$$\int_0^\infty\int_0^\infty \varphi(x^m+y^n+z^p)\,dx\,dy = 2\,\frac{\Gamma\left(1+\frac{1}{m}\right).\Gamma\left(1+\frac{1}{n}\right)}{\Gamma\left(\frac{1}{m}+\frac{1}{n}\right)}\int_0^\infty \varphi(v^2+z^p)\,v^{\frac{2}{m}+\frac{2}{n}-1}\,dv;$$

also bietet sich zunächst folgende Umformungsgleichung dar:

$$\int_0^\infty\int_0^\infty\int_0^\infty \varphi(x^m+y^n+z^p)\,dx\,dy\,dz$$

$$= 2\,\frac{\Gamma\left(1+\frac{1}{m}\right).\Gamma\left(1+\frac{1}{n}\right)}{\Gamma\left(\frac{1}{m}+\frac{1}{n}\right)}\int_0^\infty\int_0^\infty \varphi(v^2+z^p)\,v^{\frac{2}{m}+\frac{2}{n}-1}\,dv\,dz.$$

Wird nun im Doppel-Integrale rechterhand

$$v^2 \text{ durch } v^{\frac{mn}{m+n}}, \text{ also } v^{\frac{2}{m}+\frac{2}{n}-1}\,dv \text{ durch } \frac{mn}{2(m+n)}$$

ersetzt, so erhält man, beachtend die Gleichheit (2.) vorhergehender Nr., folgende:

$$\int_0^\infty\int_0^\infty\int_0^\infty \varphi(x^m y^n+z^p)\,dx\,dy\,dz$$

$$= \frac{\Gamma\left(\frac{1}{m}\right).\Gamma\left(\frac{1}{n}\right)}{(m+n)\,\Gamma\left(\frac{1}{m}+\frac{1}{n}\right)}\int_0^\infty\int_0^\infty \varphi\left(v^{\frac{mn}{m+n}}+z^p\right)dv\,dz.$$

Nun hat man, gleichfalls mit Hülfe der Reductionsgleichung (α.) vorhergehender Nr.,

$$\int_0^\infty\int_0^\infty \varphi\left(v^{\frac{mn}{m+n}}+z^p\right)dv\,dz = 2\,\frac{\Gamma\left(1+\frac{1}{m}+\frac{1}{n}\right).\Gamma\left(1+\frac{1}{p}\right)}{\Gamma\left(\frac{1}{m}+\frac{1}{n}+\frac{1}{p}\right)}\int_0^\infty \varphi(v^2)\,v^{\frac{2}{m}+\frac{2}{n}+\frac{2}{p}-1}\,dv,$$

oder auch, beachtend die Gleichheit (2.) vorhergehender Nr., folgende Gleichung:

$$\int_0^\infty \int_0^\infty \varphi(v^{\frac{mn}{m+n}} + z^p)\, dv\, dz$$

$$= 2\frac{(m+n)\,\Gamma\left(\frac{1}{m}+\frac{1}{n}\right).\Gamma\left(\frac{1}{p}\right)}{mnp\,\Gamma\left(\frac{1}{m}+\frac{1}{n}+\frac{1}{p}\right)}\int_0^\infty \varphi(v^2)\, v^{\frac{2}{m}+\frac{2}{n}+\frac{2}{p}-1}\, dv;$$

also ist

$$\int_0^\infty \int_0^\infty \int_0^\infty \varphi(x^m + y^n + z^p)\, dx\, dy\, dz$$

$$= 2\frac{\Gamma\left(\frac{1}{m}\right).\Gamma\left(\frac{1}{n}\right).\Gamma\left(\frac{1}{p}\right)}{mnp\,\Gamma\left(\frac{1}{m}+\frac{1}{n}+\frac{1}{p}\right)}\int_0^\infty \varphi(v^2)\, v^{\frac{2}{m}+\frac{2}{n}+\frac{2}{p}-1}\, dv,$$

oder endlich auch

$$(\beta.)\quad \int_0^\infty \int_0^\infty \int_0^\infty \varphi(x^m + y^n + z^p)\, dx\, dy\, dz$$

$$= 2\frac{\Gamma\left(1+\frac{1}{m}\right).\Gamma\left(1+\frac{1}{n}\right).\Gamma\left(1+\frac{1}{p}\right)}{\Gamma\left(\frac{1}{m}+\frac{1}{n}+\frac{1}{p}\right)}\int_0^\infty \varphi(v^2)\, v^{\frac{2}{m}+\frac{2}{n}+\frac{2}{p}-1}\, dv,$$

welche für alle angebbaren positiven und reellen Werthe von m, n, p Bestand hat und unsere im Eingange aufgestellte Behauptung bestätigt.

3.

Stellt man, um die allgemeinste Reductionsgleichung der mehrfachen Integrale, die den bis jetzt besprochenen analog sind, zu finden, das Integral der Differentialfunction

$$\varphi(x_1^{m_1} + x_2^{m_2} + x_3^{m_3} + \ldots + x_p^{m_p})\, dx_1\, dx_2\, dx_3 \ldots dx_p,$$

wo die Integrationen sämmtliche zwischen 0 und ∞ enthaltenen reellen Werthe der Integrationsvariabeln umfassen, durch

$$\int_0^{\infty,(p)} \varphi(x_1^{m_1} + x_2^{m_2} + \ldots + x_p^{m_p})\, dx_1\, dx_1 \ldots dx_p$$

vor, so sind wir nach den gefundenen und begründeten Ergebnissen der beiden vorhergehenden Nrn. folgende allgemeine Reductionsgleichung:

$$(A.)\quad \int_0^{\infty,(p)} \varphi\{x_1^{m_1} + x_2^{m_2} + \ldots + x_p^{m_p}\}\, dx_1\, dx_2 \ldots dx_p$$

$$= 2\frac{\Gamma\left(1+\frac{1}{m_1}\right).\Gamma\left(1+\frac{1}{m_2}\right)\ldots\Gamma\left(1+\frac{1}{m_p}\right)}{\Gamma\left(\frac{1}{m_1}+\frac{1}{m_2}+\frac{1}{m_3}+\ldots+\frac{1}{m_p}\right)}\int_0^\infty \varphi(v^2)\, v^{\frac{2}{m_1}+\frac{2}{m_2}+\ldots+\frac{2}{m_p}-1}\, dv,$$

aufzustellen und zu begründen im Stande.

Diese durch Induction erlangte Reductionsgleichung beweisen wir auf die bekannte Art, indem wir von der Annahme, sie bestehe für einen bestimmten ganzen Zahlenwerth von p (welches für die Werthe $p=2$ und $p=3$ in den beiden vorhergehen Nrn. bereits erhärtet ist), ausgehen, und dann das Bestandhaben derselben auch für $p+1$ darthun; woraus dann, wie bekannt, die allgemeine Gültigkeit für jeden positiven ganzen Werth von p unmittelbar folgt.

Wir gehen zur Erreichung dieses Ziels von der folgenden Gleichung aus:

$$\int_0^{\infty,(p+1)} \varphi\{x_1^{m_1}+x_2^{m_2}+\ldots+x_p^{m_p}+x_{p+1}^{m_{p+1}}\}\,dx_1\,dx_2\ldots dx_p\,dx_{p+1}$$
$$=\int_0^{\infty}\left\{\int_0^{\infty,(p)} \varphi\{x_1^{m_1}+x_2^{m_2}+\ldots+x_p^{m_p}+x_{p+1}^{m_{p+1}}\}\,dx_1\,dx_2\ldots dx_p\right\}dx_{p+1},$$

welche, mit Beachtung des im Eingange dieser Nr. getroffenen Übereinkommens sofort als richtig erkannt wird. Wird diese durchaus identische Gleichung mittels des durch die als bestehend angenommene Gleichung $(A.)$ ausgedrückten Ergebnisses weiter umgeformt, so erhält man, wenn der Kürze wegen

$$M = 2\,\frac{\Gamma\left(1+\frac{1}{m_1}\right).\Gamma\left(1+\frac{1}{m_2}\right)\ldots\left(1+\frac{1}{m_p}\right)}{\Gamma\left(\frac{1}{m_1}+\frac{1}{m_2}+\frac{1}{m_3}+\ldots+\frac{1}{m_p}\right)}$$

gesetzt wird, folgende Gleichung:

$$\int_0^{\infty,(p+1)} \varphi\{x_1^{m_1}+x_2^{m_2}+\ldots+x_p^{m_p}+x_{p+1}^{m_{p+1}}\}\,dx_1\,dx_2\ldots dx_p\,dx_{p+1}$$
$$= M\int_0^{\infty}\int_0^{\infty} \varphi(v^2+x_{p+1}^{m_{p+1}})\,v^{\frac{2}{m_1}+\frac{2}{m_2}+\ldots+\frac{2}{m_p}-1}\,dv\,dx_{p+1};$$

so dafs es nur noch auf die weitere Reduction des Doppel-Integrals rechterhand vom Gleichheitszeichen ankommt. Wird dasselbe einstweilen durch u vorgestellt, nämlich

$$u=\int_0^{\infty}\int_0^{\infty} \varphi(v^2+x_{p+1}^{m_{p+1}})\,v^{\frac{2}{m_1}+\frac{2}{m_2}+\ldots+\frac{2}{m_p}-1}\,dv\,dx_{p+1}$$

gesetzt, so läfst sich die Bestimmung von u auf die eines einfachen bestimmten Integrals in folgender Weise zurückführen.

Wir ersetzen nämlich im Doppel-Integrale rechterhand

$$v^{\frac{2}{m_1}+\frac{2}{m_2}+\ldots+\frac{2}{m_p}} \quad \text{durch} \quad v.$$

Dies giebt unmittelbar

$$u = \tfrac{1}{2} M_1 \int_0^{\infty} \int_0^{\infty} \varphi(v^{M_1} + x_{p+1}^{m_{p+1}})\, dv\, dx_{p+1},$$

wo zur Vereinfachung der Darstellung

$$M_1 = \frac{1}{\frac{1}{m_1} + \frac{1}{m_2} + \ldots + \frac{1}{m_p}}$$

gesetzt ist; und wenn nunmehr die in Nr. 1. aufgestellte Reductionsgleichung (α.) zugezogen wird, so ist

$$u = M_1 \frac{\Gamma\left(1+\frac{1}{M_1}\right).\Gamma\left(1+\frac{1}{m_{p+1}}\right)}{\Gamma\left(\frac{1}{M_1}+\frac{1}{m_{p+1}}\right)} \int_0^{\infty} \varphi(v^2)\, v^{\frac{2}{M_1}+\frac{2}{m_{p+1}}-1}\, dv,$$

oder auch, mit Beachtung der Gleichheit (2.) in Nr. 1.,

$$u = \frac{\Gamma\left(\frac{1}{M_1}\right).\Gamma\left(1+\frac{1}{m_{p+1}}\right)}{\Gamma\left(\frac{1}{M_1}+\frac{1}{m_{p+1}}\right)} \int_0^{\infty} \varphi(v^2)\, v^{\frac{2}{M_1}+\frac{2}{m_{p+1}}-1}\, dv.$$

Die für u gefundene Bestimmung in die oben aufgestellte Gleichung gesetzt, giebt

$$\int_0^{\infty,(p+1)} \varphi\{x_1^{m_1} + x_2^{m_2} + \ldots + x_p^{m_p} + x_{p+1}^{m_{p+1}}\}\, dx_1\, dx_2 \ldots dx_p\, dx_{p+1}$$

$$= M \frac{\Gamma\left(\frac{1}{M_1}\right).\Gamma\left(1+\frac{1}{m_{p+1}}\right)}{\Gamma\left(\frac{1}{M_1}+\frac{1}{m_{p+1}}\right)} \int_0^{\infty} \varphi(v^2)\, v^{\frac{2}{M_1}+\frac{2}{m_{p+1}}-1}\, dv,$$

und wenn hier die Werthe für M und M_1 restituirt werden, so ergiebt sich endlich die Gleichung

$$\int_0^{\infty,(p+1)} \varphi\{x_1^{m_1} + x_2^{m_2} + \ldots + x_p^{m_p} + x_{p+1}^{m_{p+1}}\}\, dx_1\, dx_2 \ldots dx_p\, dx_{p+1}$$

$$= 2 \frac{\Gamma\left(1+\frac{1}{m_1}\right).\Gamma\left(1+\frac{1}{m_2}\right)\ldots\Gamma\left(1+\frac{1}{m_{p+1}}\right)}{\Gamma\left(\frac{1}{m_1}+\frac{1}{m_2}+\ldots+\frac{1}{m_{p+1}}\right)} \int_0^{\infty} \varphi(v^2)\, v^{\frac{2}{m_1}+\frac{2}{m_2}+\ldots+\frac{2}{m_{p+1}}-1}\, dv,$$

welche, mit der durch Induction erlangten Reductionsgleichung (A.) verglichen, die Richtigkeit unserer Behauptung unzweideutigerweise darthut. *Es gilt also die allgemeine Reductionsgleichung* (A.) *für alle ganzen und positiven Werthe von p, wenn die Exponenten der Integrationsvariabeln*, d. h. *die constanten Gröfsen*

$$m_1,\ m_2,\ m_3,\ \ldots\ m_p,$$

positive reelle Werthe haben.

4.

Aus der in vorhergehender Nr. aufgestellten und begründeten Reductionsgleichung (*A.*) leiten wir noch auf folgendem Wege eine bei weitem allgemeinere ab.

Werden in derselben zuerst die Integrationsvariabeln des *p*fachen Integrals, nämlich die Gröfsen

$$x_1,\ x_2,\ x_3,\ \ldots\ x_p$$

nach der Ordnung ihrer Folge durch

$$x_1^{\frac{1}{m_1}},\ x_2^{\frac{1}{m_2}},\ x_3^{\frac{1}{m_3}},\ \ldots\ x_p^{\frac{1}{m_p}}$$

ersetzt, so geht die Reductionsgleichung, mit Zuziehung der Gleichheit (2.) in Nr. 1., in folgende über:

$$\int_0^{\infty,(p)} \varphi\{x_1+x_2+\ldots+x_p\}\, x_1^{\frac{1}{m_1}-1}.x_2^{\frac{1}{m_2}-1}\ldots x_p^{\frac{1}{m_p}-1}\, dx_1\, dx_2 \ldots dx_p$$

$$= 2\frac{\Gamma\left(\frac{1}{m_1}\right).\Gamma\left(\frac{1}{m_2}\right)\ldots\Gamma\left(\frac{1}{m_p}\right)}{\Gamma\left(\frac{1}{m_1}+\frac{1}{m_2}+\ldots+\frac{1}{m_p}\right)}\int_0^{\infty}\varphi(v^2)v^{2\left(\frac{1}{m_1}+\frac{1}{m_2}+\ldots+\frac{1}{m_p}\right)-1}dv.$$

Ersetzt man hier die reellen und positiven angebbaren Constanten $m_1, m_2, \ldots m_p$ durch die reciproken Werthe derselben, so erhält man die Reductionsgleichung

$$\int_0^{\infty,(p)} \varphi\{x_1+x_2+\ldots+x_p\}\, x_1^{m_1-1}.x_2^{m_2-1}\ldots x_p^{m_p-1}\, dx_1\, dx_2 \ldots dx_p$$

$$= 2\frac{\Gamma(m_1).\Gamma(m_2)\ldots\Gamma(m_p)}{\Gamma(m_1+m_2+\ldots+m_p)}\int_0^{\infty}\varphi(v^2)\,v^{2(m_1+m_2+\ldots+m_p)-1}dv,$$

in welcher die Exponenten $m_1, m_2, m_3, \ldots m_p$, wie bisher, reelle und positive angebbare Gröfsen sind. Wenn nun endlich in dieser Reductionsgleichung die Integrationsvariabeln

$$x_1,\ x_2,\ x_3,\ \ldots\ x_p$$

der Reihe nach in

$$a_1x_1^{n_1},\ a_2x_2^{n_2},\ a_3x_3^{n_3},\ \ldots\ a_px_p^{n_p}$$

übergehen, wo die Coëfficienten sowohl als die Exponenten, nämlich

$$a_1,\ a_2,\ a_3,\ \ldots\ a_p,\qquad n_1,\ n_2,\ n_3,\ \ldots\ n_p,$$

reelle und positive angebbare Constanten sind, und wenn hierauf die vorhin erwähnten Exponenten

$$m_1,\ m_2,\ m_3,\ \ldots\ m_p$$

nach der Ordnung ihrer Folge durch



$$\frac{r_1}{n_1}, \frac{r_2}{n_2}, \frac{r_3}{n_3}, \ldots \frac{r_p}{n_p}$$

ersetzt werden, wo also $r_1, r_2, r_3, \ldots r_p$ ebenfalls reelle und positive angebbare Constanten sind; so stellt sich die am Eingange dieser Abhandlung angekündigte Reductionsgleichung wie folgt dar:

$$\text{(I.)} \int_0^{\infty,(p)} \varphi\{a_1 x_1^{n_1} + a_2 x_2^{n_2} + \ldots + a_p x_p^{n_p}\} x_1^{r_1-1} . x_2^{r_2-1} \ldots x_p^{r_p-1} dx_1\, dx_2 \ldots dx_p$$

$$= N \int_0^{\infty} \varphi(v^2)\, v^{2\left(\frac{r_1}{n_1} + \frac{r_2}{n_2} + \ldots + \frac{r_p}{n_p}\right)-1} dv,$$

wo zur Vereinfachung

$$\text{(II.)} \quad N = \frac{2}{n_1 n_2 \ldots n_p\, a_1^{\frac{r_1}{n_1}} a_2^{\frac{r_2}{n_2}} \ldots a_p^{\frac{r_p}{n_p}}} . \frac{\Gamma\left(\frac{r_1}{n_1}\right) \Gamma\left(\frac{r_2}{n_2}\right) \ldots \Gamma\left(\frac{r_p}{n_p}\right)}{\left(\frac{r_1}{n_1} + \frac{r_2}{n_2} + \ldots + \frac{r_p}{n_p}\right)}$$

gesetzt worden ist. Diese Reductionsgleichung besteht für jeden ganzen und positiven Werth von p und die Constanten

$$a_1, a_2, a_3, \ldots a_p, \quad r_1, r_2, \ldots r_p, \quad n_1, n_2, \ldots n_p$$

sind alle reeller, jedoch nur positiv angebbarer Werthe fähig; die Function φ endlich bleibt ganz willkürlich.

Zürich, im April 1843.

4.

Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Criterien des cubischen Characters der Zahl 3 und ihrer Theiler.

(Von Herrn Stud. G. *Eisenstein* zu Berlin.)

Wir haben gesehen (4tes Heft 27ten Bandes d. Journ.), dafs die Frage nach dem cubischen Character jeder ganzen complexen Zahl immer auf eine einfachere Aufgabe zurückgeführt werden kann, bei welcher es sich nur um den cubischen Character von *Primzahlen* handelt. Ist nemlich M eine beliebig gegebene ganze complexe Zahl, so kann man immer

$$M = (-1)^{\lambda} \varrho^{\mu} (1-\varrho)^{\nu} f^{\alpha} f'^{\beta} f''^{\gamma} \ldots.$$

setzen, wo alle Exponenten positive ganze Zahlen sind, während $f, f', f'', \ldots$ primäre complexe Primzahlen bezeichnen; und dann hat man, nach einem in der Abhandlung (§. 2.) bewiesenen Satze,

$$\left[\frac{M}{l}\right] = \left[\frac{-1}{l}\right]^{\lambda} \left[\frac{\varrho}{l}\right]^{\mu} \left[\frac{1-\varrho}{l}\right]^{\nu} \left[\frac{f}{l}\right]^{\alpha} \left[\frac{f'}{l}\right]^{\beta} \left[\frac{f''}{l}\right]^{\gamma},$$

wo l einen gegebenen Modul bezeichnet, der immer primär, d. h. $\equiv -1 \pmod{3}$, und nicht in M aufgehend angenommen werden soll. Es bleiben also nur *vier* Fragen zu lösen, nämlich, Criterien des cubischen Characters anzugeben:

1) für die Zahl -1,
2) für die complexe Einheit ϱ,
3) für $1-\varrho$, und endlich
4) für die primären complexen Primzahlen.

Die erste Aufgabe findet sich sofort gelöset, da, wegen $(-1)^3 = -1$, immer $\left[\frac{-1}{l}\right] = 1$ ist. Die Lösung der zweiten Aufgabe giebt die Formel

$$\left[\frac{\varrho}{l}\right] = \varrho^{\frac{1}{3}(N(l)-1)},$$

welche sich unmittelbar aus der Definition des symbolischen Zeichens ergiebt. Sie läfst sich in folgendem Satze aussprechen:

„Der cubische Character von ϱ in Beziehung auf die primäre complexe Primzahl l ist 0, 1 oder 2, je nachdem die Norm von l von der Form $9n+1$, $9n+4$ oder $9n+7$ ist."

Die vierte der obigen Aufgaben wird durch das Reciprocitätsgesetz gelöset, nemlich durch den Satz:

„Wenn $l \equiv l' \equiv -1$ (mod. 3.) zwei primäre complexe Primzahlen mit verschiedener Norm sind, so ist $\left[\frac{l'}{l}\right] = \left[\frac{l}{l'}\right]$."

Wir haben den strengen und allgemeinen Beweis dieses Satzes gegeben. Aber dieser Satz lehrt nichts in Beziehung auf die Zahl 3 und ihre Theiler. Es bleibt also zur Vervollständigung der Theorie der cubischen Charactere noch die Lösung der dritten Aufgabe übrig, d. h. es ist ein Satz aufzustellen, welcher die Criterien giebt, nach denen auf eine einfache Weise alle primären Primzahlen l in drei Classen getheilt werden können, je nachdem für dieselben $\left[\frac{1-\varrho}{l}\right] = 1$, oder $= \varrho$, oder $= \varrho^2$ ist. Soviel mir bekannt, fehlt noch dieser Satz, obgleich derselbe zu einer vollständigen Theorie unentbehrlich ist; die Primzahl $1-\varrho$ spielt hier dieselbe Rolle, wie die Zahl 2 in der Theorie der quadratischen Reste. Durch die folgenden Betrachtungen wird man zu dem gewünschten Ziele gelangen. Es ist $(1-\varrho)^2 = 1 - 2\varrho + \varrho^2 = -3\varrho$, also

$$\left[\frac{1-\varrho}{l}\right]^2 = \left[\frac{3}{l}\right]\left[\frac{\varrho}{l}\right] = \left[\frac{3}{l}\right].\varrho^{\frac{1}{3}(N(l)-1)} \text{ und}$$

$$\left[\frac{1-\varrho}{l}\right] = \left[\frac{3}{l}\right]^2.\varrho^{\frac{2}{3}(N(l)-1)}.$$

Ist nun zuerst l eine reelle Primzahl $3n+2$, so ist $\left[\frac{3}{l}\right] = 1$, also ganz einfach

$$\left[\frac{1-\varrho}{l}\right] = \varrho^{\frac{2}{3}(N(l)-1)}.$$

Ist aber l eine zweigliedrige primäre Primzahl $= a + b\varrho$, so hängt die Bestimmung des Werths von $\left[\frac{1-\varrho}{l}\right]$ von dem des Ausdrucks $\left[\frac{3}{l}\right]$ ab. Dieser letztere nun wird durch folgenden Lehrsatz gefunden.

„Wenn $l = a + b\varrho$ eine primäre complexe Primzahl ist, so daſs also $a \equiv -1$ (mod. 3), $b \equiv 0$ (mod. 3) ist, so hat man

$$\left[\frac{3}{a+b\varrho}\right] = \varrho^{\frac{1}{3}l},$$

oder

$$\left[\frac{3}{l}\right] = 1 \text{ für } l \equiv 2,\ 5,\ 8 \text{ (mod. 9)},$$

$$\left[\frac{3}{l}\right] = \varrho, \text{ für } l \equiv 2+6\varrho,\ 5+6\varrho,\ 8+6\varrho \text{ (mod. 9)},$$

$$\left[\frac{3}{l}\right] = \varrho^2, \text{ für } l \equiv 2+3\varrho,\ 5+3\varrho,\ 8+3\varrho \text{ (mod. 9)}."$$

Der Beweis dieses Satzes folgt am Schlusse dieser Abhandlung.

Wenn man nun $a = 3m - 1$, $b = 3n$ setzt, so folgt $N(l) = a^2 - ab + b^2 = 9m^2 - 6m + 1 - 9mn + 3n + 9n^2 \equiv 3(m+n)+1 \pmod{9}$, folglich $\frac{1}{3}(N(l) - 1) \equiv m + n \pmod{3}$. Es ist demnach

$$\left[\frac{\varrho}{l}\right] = \varrho^{m+n}, \quad \left[\frac{3}{l}\right] = \varrho^{2n}, \quad \left[\frac{1-\varrho}{l}\right] = \varrho^{2m+2n} \cdot \varrho^{n} = \varrho^{2m} = \varrho^{\frac{2}{3}(a+1)}.$$

„Ist l eine primäre complexe Primzahl $= a + b\varrho$, so ist $\left[\frac{1-\varrho}{a+b\varrho}\right] = \varrho^{\frac{2}{3}(a+1)}$, nämlich

$$\left[\frac{1-\varrho}{l}\right] = 1, \quad \text{wenn } l \equiv 8,\ 8+3\varrho,\ 8+6\varrho \pmod{9},$$

$$\left[\frac{1-\varrho}{l}\right] = \varrho, \quad \text{wenn } l \equiv 5,\ 5+3\varrho,\ 5+6\varrho \pmod{9},$$

$$\left[\frac{1-\varrho}{l}\right] = \varrho^2, \quad \text{wenn } l \equiv 2,\ 2+3\varrho,\ 2+6\varrho \pmod{9};$$

und dieser Satz gilt auch, wenn l eine eingliedrige Primzahl ist."

Die bisher für Primzahlen bewiesenen Sätze lassen sich, eben so wie das Reciprocitätsgesetz, auf primäre zusammengesetzte Zahlen ausdehnen. Ist nemlich $L = A + B\varrho$ irgend eine primäre complexe Zahl, so behaupte ich, dafs, ganz wie für Primzahlen,

$$\left[\frac{\varrho}{L}\right] = \varrho^{\frac{1}{3}(N(L)-1)}, \quad \left[\frac{\varrho}{L}\right] = \varrho^{\frac{1}{3}(A+B+1)},$$

$$\left[\frac{3}{L}\right] = \varrho^{\frac{2}{3}B}, \quad \left[\frac{1-\varrho}{L}\right] = \varrho^{\frac{2}{3}(A+1)}$$

sein wird. Es leuchtet ein, dafs diese Formeln bewiesen sein werden, sobald sich zeigen läfst, dafs sie für die primäre Zahl $-LL'$ gelten, wenn sie für die beiden primären Zahlen L und L' richtig sind; denn da sie für primäre Primzahlen gelten, so werden sie dann auch für primäre zusammengesetzte Zahlen ihre Gültigkeit behalten. Man nehme also an, dafs die obigen Formeln für die beiden Nenner L, L' bewiesen seien, und suche sie aus dieser Annahme für den Nenner $-LL'$ abzuleiten. Was die erste Formel betrifft, so ist nach der Annahme

$$\left[\frac{\varrho}{L}\right] = \varrho^{\frac{1}{3}(N(L)-1)}, \quad \left[\frac{\varrho}{L'}\right] = \varrho^{\frac{1}{3}(N(L')-1)},$$

also, wenn man $N(L) = 3\mu + 1$, $N(L') = 3\mu' + 1$ setzt,

$$\left[\frac{\varrho}{L}\right]\left[\frac{\varrho}{L'}\right] = \left[\frac{\varrho}{-LL'}\right] = \varrho^{\mu+\mu'}.$$

Aber es ist $N(L)N(L') = 9\mu\mu' + 3\mu + 3\mu' + 1 \equiv 3(\mu+\mu')+1 \pmod{9}$, also



ist $\frac{1}{3}(N(LL')-1) \equiv \mu + \mu'$ (mod. 3), und folglich auch $\left[\frac{\varrho}{-LL'}\right] = \varrho^{\frac{1}{3}(N(LL')-1)}$; was zu beweisen war.

Um die übrigen Formeln zu beweisen, setze man $L = A + B\varrho$ und $L' = A' + B'\varrho$, so dafs $-LL' = A'' + B''\varrho$, $A'' = BB' - AA'$, $B'' = BB' - AB' - A'B$ wird; ferner setze man $A = 3m - 1$, $B = 3n$, $A' = 3m' - 1$, $B' = 3n'$, $A'' = 3m'' - 1$, $B'' = 3n''$, so ist

$$A'' = 9nn' - 9mm' + 3m + 3m' - 1 \equiv 3(m + m') - 1 \pmod{9},$$
$$B'' = 9nn' - 9m'n + 3n - 9mn' + 3n' \equiv 3(n + n') \pmod{9},$$

folglich $m + m' \equiv m''$ (mod. 3) und $n + n' \equiv n''$ (mod. 3).

Ist also nach der Voraussetzung

$$\left[\frac{\varrho}{L}\right] = \varrho^{m+n}, \quad \left[\frac{\varrho}{L'}\right] = \varrho^{m'+n'},$$
$$\left[\frac{3}{L}\right] = \varrho^{2n}, \quad \left[\frac{3}{L'}\right] = \varrho^{2n'},$$
$$\left[\frac{1-\varrho}{L}\right] = \varrho^{2m}, \quad \left[\frac{1-\varrho}{L'}\right] = \varrho^{2m'},$$

so folgt hieraus

$$\left[\frac{\varrho}{-LL'}\right] = \varrho^{m+m'+n+n'} = \varrho^{m''+n''},$$
$$\left[\frac{3}{-LL'}\right] = \varrho^{2n+2n'} = \varrho^{2n''},$$
$$\left[\frac{1-\varrho}{-LL'}\right] = \varrho^{2m+2m'} = \varrho^{2m''};$$

was zu beweisen war.

Es ist gut für die Ausübung, zu bemerken, dafs das Reciprocitätsgesetz für Primzahlen auch dann noch gilt, wenn die beiden Primzahlen zweigliedrig sind und zu *derselben Norm* gehören. Sind nämlich $a + b\varrho$, $a + b\varrho^2$ zwei zweigliedrige *conjugirte* complexe Primzahlen, wo a und b von 0 verschieden und, wie immer, $b \equiv 0$ (mod. 3) vorausgesetzt wird, so hat man $\left[\frac{a+b\varrho}{a+b\varrho^2}\right] = \left[\frac{a+b\varrho^2}{a+b\varrho}\right] = 1$. Um sich davon zu überzeugen, genügt es, die beiden Congruenzen

$$a(a + b\varrho) \equiv a^2 - b^2 \pmod{a + b\varrho^2}, \quad a(a + b\varrho^2) \equiv a^2 - b^2 \pmod{a + b\varrho}$$

aufzustellen, aus denen nach und nach

$$\left[\frac{a+b\varrho}{a+b\varrho^2}\right] = \left[\frac{a}{a+b\varrho^2}\right]^2 \left[\frac{a^2-b^2}{a+b\varrho^2}\right], \quad \left[\frac{a+b\varrho^2}{a+b\varrho}\right] = \left[\frac{a}{a+b\varrho}\right]^2 \left[\frac{a^2-b^2}{a+b\varrho}\right],$$

$$\left[\frac{a+b\varrho^2}{a+b\varrho}\right]^2 = \left[\frac{a}{a+b\varrho^2}\right]^2\left[\frac{a^2-b^2}{a+b\varrho^2}\right], \qquad \left[\frac{a+b\varrho}{a+b\varrho^2}\right]\left[\frac{a+b\varrho^2}{a+b\varrho}\right]^2 =$$
$$\left[\frac{a}{a+b\varrho^2}\right]\left[\frac{a^2-b^2}{(a+b\varrho^2)^2}\right] = \left[\frac{a+b\varrho^2}{a}\right]\left[\frac{a^2-b^2+(2ab-b^2)\varrho^2}{a^2-b^2}\right] =$$
$$\left[\frac{b\varrho^2}{a}\right]\left[\frac{(2ab-b^2)\varrho^2}{a^2-b^2}\right] = \left[\frac{\varrho^2}{a}\right]\left[\frac{\varrho^2}{a^2-b^2}\right] = \left[\frac{\varrho}{a^2}\right]\left[\frac{\varrho}{a^2-b^2}\right]^2 = \left[\frac{\varrho}{a^2}\right]^3 = 1$$

folgt. Von der andern Seite ist $\left[\frac{a+b\varrho}{a+b\varrho^2}\right] = \left[\frac{a+b\varrho^2}{a+b\varrho}\right]^2$, folglich $\left[\frac{a+b\varrho}{a+b\varrho^2}\right] = \left[\frac{a+b\varrho^2}{a+b\varrho}\right] = 1$. Bei dem einfachen und folglich auch bei dem verallgemeinerten Reciprocitätssatze kann demnach die Bedingung wegfallen, welche erfordert, dafs die *Normen* der beiden complexen Zahlen relative Primzahlen zu einander sein sollen. Wenn also die imaginären Theile der beiden complexen Zahlen P und Q durch 3 theilbar und sie selbst relative Primzahlen zu einander sind, so wird immer $\left[\frac{P}{Q}\right] = \left[\frac{Q}{P}\right]$ sein, die Normen von P und Q mögen gemeinschaftliche Theiler haben, oder nicht. Diese Ergänzung ist nöthig, weil man nun allgemein den Werth von $\left[\frac{P}{Q}\right]$ blofs mit Hülfe eines Divisions-Schemas, d. h. mittels derselben Operation, welche man anwendet, um den gröfsten gemeinschaftlichen Theiler von P und Q zu berechnen, mit der gröfsten Leichtigkeit finden kann, ohne darauf achten zu müssen, ob die Norm jedes Restes zu der Norm des vorhergehenden Divisors relative Primzahl sei. Man vergleiche „Einfacher Algorithmus zur Bestimmung des Werthes von $\left(\frac{a}{b}\right)$" im 4ten Hefte des 27ten Bandes dieses Journals

Wir geben jetzt schliefslich den Beweis des oben aufgestellten Satzes über die Criterien des cubischen Characters der Zahl 3.

Beweis. Wenn p eine reelle Primzahl $3n+1$ ist und $p_1 = a+b\varrho$, $p_2 = a+b\varrho^2$ ihre beiden primären complexen Primfactoren sind, also $p_1 \equiv p_2 \equiv 2 \pmod{3}$ ist; wenn ferner r eine imaginäre $p$te Wurzel der Einheit und t eine beliebige, nicht durch p theilbare ganze Zahl vorstellt, so hatten wir oben gefunden („Beweis des cubischen Reciprocitätsgesetzes"):

$$\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right]r^k = \eta = \sqrt[3]{(pp_1)}, \qquad \Sigma\left[\frac{k^2}{p_1}\right]r^k = \vartheta = \sqrt[3]{(pp_2)},$$
$$\Sigma\left[\frac{k}{p_1}\right]r^{tk} = \left[\frac{t^2}{p_1}\right]\eta, \qquad \Sigma\left[\frac{k^2}{p_1}\right]r^{tk} = \left[\frac{t}{p_1}\right]\vartheta,$$

wo sich alle Summationen von $k=1$ bis $k=p-1$ erstrecken, und wo die

beiden Cubikwurzeln so zu nehmen sind, dafs ihr Product $\eta\vartheta = p$ wird. Bezeichnet man durch P_0, P_1, P_2 den Inbegriff derjenigen Wurzeln r^k, für welche resp. $\left[\frac{k}{p_1}\right] = 1$, ϱ oder ϱ^2 ist, so dafs P_0, P_1, P_2 die drei ***Perioden*** (nach ***Gaufs***) sind, in welche die Gesammtheit der Wurzeln Ω der Gleichung

$$\frac{x^p - 1}{x - 1} = 0$$

zerfällt, so kann man die drei Gleichungen aufstellen:

$$P_0 + \varrho P_1 + \varrho^2 P_2 = \eta, \quad P_0 + \varrho^2 P_1 + \varrho P_2 = \vartheta, \quad P_0 + P_1 + P_2 = -1.$$

Löset man diese drei Gleichungen nach P_0, P_1, P_2 als den Unbekannten auf, so findet sich

$$P_0 = \tfrac{1}{3}[-1 + \eta + \vartheta], \quad P_1 = \tfrac{1}{3}[-1 + \varrho^2\eta + \varrho\vartheta], \quad P_2 = \tfrac{1}{3}[-1 + \varrho\eta + \varrho^2\vartheta].$$

Ebenso findet man, wenn S_t die Summe der $t$ten Potenzen der in der Periode P_0 enthaltenen Wurzeln bezeichnet,

$$S_t = \tfrac{1}{3}\left[-1 + \left[\frac{t^2}{p_1}\right]\eta + \left[\frac{t}{p_1}\right]\vartheta\right].$$

Betrachten wir die Gleichung vom Grade $\frac{1}{3}(p-1)$, deren Wurzeln die in der Periode P_0 enthaltenen Wurzeln der Einheit sind. Es sei diese Gleichung

$$x^{\frac{1}{3}(p-1)} + K_1 x^{\frac{1}{3}(p-1)-1} + K_2 x^{\frac{1}{3}(p-1)-2} + \text{etc.} = 0.$$

Die Coëfficienten dieser Gleichung werden alle von der Form

$$AP_0 + BP_1 + CP_2$$

sein, wo ***A, B, C reelle ganze*** Zahlen sind: also werden sie auch auf die Form

$$\tfrac{1}{3}(D + E\eta + F\vartheta),$$

gebracht werden können, wo ***D, E, F complexe ganze*** Zahlen sind.

Nach dem *Newton*schen Lehrsatze kann man nun die ***Coëfficienten*** einer Gleichung durch die ***Potenzensummen*** der Wurzeln ausdrücken. Es ist nach diesem Satze

$$K_1 = -S_1, \quad 2K_2 = -K_1 S_1 - S_2 = S_1^2 - S_2,$$

$$3K_3 = -K_2 S_1 - K_1 S_2 - S_3 = \tfrac{1}{2}(3S_1 S_2 - S_1^3 - 2S_3) \text{ u. s. w.}$$

Setzt man allgemein

$$K_t = \tfrac{1}{3}(D_t + E_t\eta + F_t\vartheta),$$

führt in die eben erhaltenen Gleichungen statt S_1, S_2, S_3 u. s. w. ihre vorhin gefundenen Werthe ein und bemerkt noch, dafs $\eta\vartheta = p$, $\eta^2 = p_1\vartheta$, $\vartheta^2 = p_2\eta$, $\vartheta^3 = pp_1$, $\eta^3 = pp_2$ ist, so kommt

$$D_1 = 1, \quad E_1 = -1, \quad F_1 = -1,$$

$$D_2 = \tfrac{1}{3}(p+2), \quad E_2 = \tfrac{1}{3}\left(p_2 - 2 - 3\left[\frac{4}{p_1}\right]\right), \quad F_2 = \tfrac{1}{3}\left(p_1 - 2 - 3\left[\frac{2}{p_1}\right]\right),$$

$$D_3 = \frac{1}{2.27}\left\{28 + 6p - pp_1 - pp_2 + 9p\left[\frac{4}{p_1}\right] + 9p\left[\frac{2}{p_1}\right]\right\},$$

$$E_3 = \frac{1}{2.27}\left\{-12 - 3p + 3p_2 - 9\left[\frac{4}{p_1}\right] + 9p_2\left[\frac{2}{p_1}\right] - 18\left[\frac{3}{p_2}\right]\right\},$$

$$F_3 = \frac{1}{2.27}\left\{-12 - 3p + 3p_1 - 9\left[\frac{2}{p_1}\right] + 9p_1\left[\frac{4}{p_1}\right] - 18\left[\frac{3}{p_1}\right]\right\},$$

u. s. w.

Die Gleichung für F_3 beweiset, daſs $p_1 - 2 - 3\left[\frac{2}{p_1}\right]$ durch 6 theilbar ist; man hat also $p_1 \equiv 3\left[\frac{2}{p_1}\right] \equiv \left[\frac{2}{p_1}\right]$ (mod. 2), d. h. es ist $\left[\frac{2}{p_1}\right] = 1$, ρ oder ρ^2, je nachdem $p_1 \equiv 1$, ρ oder ρ^2 (mod. 2) ist: d. h. es ist $\left[\frac{2}{p_1}\right] = \left[\frac{p_1}{2}\right]$: wie aus dem Reciprocitätsgesetze folgte, aber jetzt auf einem neuen Wege gefunden wurde.

Die Formel für F_3 beweiset, daſs

$$-4 - p + p_1 - 3\left[\frac{2}{p_1}\right] + 3p_1\left[\frac{4}{p_1}\right] - 6\left[\frac{3}{p_1}\right] \equiv 0 \pmod{9}.$$

Erwägt man, daſs $p_1 \equiv -1$ (mod. 3), also $3p_1 \equiv -3$ (mod. 9) ist, und daſs $\left[\frac{2}{p_1}\right] + \left[\frac{4}{p_1}\right]$ nur entweder $= -1$ oder $= 2$ sein kann, also immer $\equiv -1$ (mod. 3) ist, so erhält man $-3\left[\frac{2}{p_1}\right] + 3p_1\left[\frac{4}{p_1}\right] \equiv 3$ (mod. 9); folglich geht die obige Congruenz über in:

$$-1 - p + p_1 - 6\left[\frac{3}{p_1}\right] \equiv 0 \pmod{9} \quad \text{oder}$$

$$\tfrac{1}{3}(-1 - p + p_1) \equiv 2\left[\frac{3}{p_1}\right] \pmod{3}, \quad \left[\frac{3}{p_1}\right] \equiv \tfrac{1}{3}(p + 1 - p_1) \pmod{3}.$$

Setzt man daher $p_1 = a + b\rho$, $a = 3\alpha + 2$, $b = 3\beta$, so hat man $\left[\frac{3}{p_1}\right] \equiv \frac{1}{3}(p-1) - \alpha - \beta\rho$ (mod. 3). Ferner ist

$$p = a^2 - ab + b^2 = 9\alpha^2 + 12\alpha + 4 - 9\alpha\beta - 6\beta + 9\beta^2 \equiv 3\alpha + 3\beta + 4 \pmod{9},$$

also ist

$$\tfrac{1}{3}(p - 1) \equiv \alpha + \beta + 1 \pmod{3}.$$

Verbindet man diese Congruenz mit der vorigen, so kommt

$$\left[\frac{3}{p_1}\right] \equiv 1 + \beta(1 - \rho) \pmod{3}.$$

Also erhält man, je nachdem $\beta \equiv 0, 1, 2$ (mod. 3) ist,

$$\left[\frac{3}{p_1}\right] \equiv 1, \rho^2, \rho \pmod{3};$$

was nicht anders geschehen kann, als wenn in den drei Fällen resp.

$\left[\frac{3}{p_1}\right] = 1,\ \varrho^2,\ \varrho$ ist: also ist in allen Fällen

$$\left[\frac{3}{p_1}\right] = \varrho^{2\beta}; \quad \text{was zu beweisen war.}$$

Setzt man die obigen Formeln für die verschiedenen D, E, F beliebig weiter fort, so kann man auf demselben Wege eine Reihe von beliebig vielen Lehrsätzen ableiten. Das hier angewandte Princip ist aber auch für die Theorie der höheren Potenzenreste von Wichtigkeit und liefert namentlich die Ergänzungssätze, welche in den allgemeinen Reciprocitätsgesetzen nicht enthalten sind. Auf diese Weise erhält man z. B. mit der gröfsten Leichtigkeit den Satz, welchen *Gaufs* in den 9 letzten Paragraphen seiner zweiten Abhandlung über die biquadratischen Reste bewiesen hat.

Anmerkung. In der Seite 282 drittes Heft 27ten Bandes von mir aufgestellten Formel befindet sich ein Druckfehler. Die Formel heifst nemlich:

$$p\left\{\frac{\operatorname{tang}\frac{p\pi}{q}}{\operatorname{tang}\frac{2\pi}{q}} + \frac{\operatorname{tang}\frac{2p\pi}{q}}{\operatorname{tang}\frac{4\pi}{q}} + \dots + \frac{\operatorname{tang}\frac{\frac{1}{2}(q-1)p\pi}{q}}{\operatorname{tang}\frac{(q-1)\pi}{q}}\right\}$$

$$+q\left\{\frac{\operatorname{tang}\frac{q\pi}{p}}{\operatorname{tang}\frac{2\pi}{p}} + \frac{\operatorname{tang}\frac{2q\pi}{p}}{\operatorname{tang}\frac{4\pi}{p}} + \dots + \frac{\operatorname{tang}\frac{\frac{1}{2}(p-1)q\pi}{p}}{\operatorname{tang}\frac{(p-1)\pi}{p}}\right\} = -\tfrac{1}{4}(p-q)^2;$$

dort steht rechts unrichtigerweise $-\frac{1}{2}(p-q)^2$.

Einen Druckfehler, der sich im zweiten Hefte auf Seite 106 befindet, bitte ich ebenfalls zu verbessern. Dort ist vor $a\Delta^2$, $b\Delta^2$, $c\Delta^2$, $d\Delta^2$ das Zeichen — weggelassen worden.

5.

Transformations remarquables de quelques séries.

(Par Mr. G. *Eisenstein* à Berlin.)

(Suite de l'article No. 14. tome 27. de ce journal. Cet article commence cah. 3. tome 27.)

Nouveaux développements des fonctions elliptiques.

En posant $K=\int_0^{\frac{1}{2}\pi}\frac{d\varphi}{\sqrt{(1-k^2\sin^2\varphi)}}$, $K'=\int_0^{\frac{1}{2}\pi}\frac{d\varphi}{\sqrt{(1-k'^2\sin^2\varphi)}}$, $k^2+k'^2=1$, $p=e^{\pi\frac{K'}{K}}$, on a les formules très simples:

$$\sqrt{\left(\frac{2K}{\pi}\right)} = 1+\cfrac{2}{p-\cfrac{p}{p^3+1-\cfrac{p^3}{p^5+1-\cfrac{p^5}{p^7+1-\text{etc.}}}}}$$

$$\sqrt{\left(\frac{2k'K}{\pi}\right)} = 1-\cfrac{2}{p+\cfrac{p}{p^3-1+\cfrac{p^3}{p^5-1+\cfrac{p^5}{p^7-1+\text{etc.}}}}}$$

On peut donc exprimer *le carré* de la première fraction continue par une autre fraction continue d'une loi également très simple, c'est à dire par la suivante:

$$1+4p:(1+p^2-p(1+p^2)^2:(1+p^4+p^3(1-p^2)^2:(1+p^6-p^3(1+p^4)^2$$
$$:(1+p^8+p^5(1-p^4)^2:(1+p^{10}-\text{etc.}))),$$

dont la valeur est $\frac{2K}{\pi}$.

En donnant aux symboles

$$\sin\text{am},\quad \cos\text{am},\quad \Delta\,\text{am},\quad \text{tang}\,\text{am}$$

la même signification qu'ils ont dans les „*Fundamenta nova*" de Mr. *Jacobi*, et en posant pour abréger,

$$\sqrt{-1}=i,\qquad z=e^{\frac{\pi x}{2K}i},\qquad p=e^{\frac{K'\pi}{K}}\quad \text{(ce qui suppose } p>1\text{)},$$

on a

$$\sin\text{am}\,x = \frac{2}{\sqrt[4]{p}\,.\sqrt{k}}\sin\frac{\pi x}{2K}.(A^2+B^2),$$

$$A+Bi = \cfrac{1}{1-\cfrac{z^2}{1+p-\cfrac{pz^2}{1+p^2-\cfrac{p^2z^2}{1+p^3-\cfrac{p^3z^2}{1+p^4-\cfrac{p^4z^2}{1+p^5-\text{etc. in inf.}}}}}}}$$

$$\cos\operatorname{am}x = \frac{2}{\sqrt[4]{p}}\sqrt{\left(\frac{k'}{k}\right)}\cos\frac{\pi x}{2K}.(C^2+D^2),$$

$$C+Di = \cfrac{1}{1+\cfrac{z^2}{1-p-\cfrac{pz^2}{1+p^2+\cfrac{p^2z^2}{1-p^3-\cfrac{p^3z^2}{1+p^4+\cfrac{p^4z^2}{1-p^5-\text{etc.}}}}}}}$$

$$\frac{\sin\operatorname{am}x}{\Delta\operatorname{am}x} = \frac{2}{\sqrt[4]{p}\,\sqrt{(kk')}}\sin\frac{\pi x}{2K}.(E^2+F^2),$$

$$E+Fi = \cfrac{1}{1-\cfrac{z^2}{1-p+\cfrac{pz^2}{1+p^2-\cfrac{p^2z^2}{1-p^3+\cfrac{p^3z^2}{1+p^4-\cfrac{p^4z^2}{1-p^5+\text{etc.}}}}}}}$$

$$\frac{\cos\operatorname{am}x}{\Delta\operatorname{am}x} = \frac{2}{\sqrt[4]{p}\,\sqrt{k}}\cos\frac{\pi x}{2K}.(G^2+H^2),$$

$$G+Hi = \cfrac{1}{1+\cfrac{z^2}{1+p+\cfrac{pz^2}{1+p^2+\cfrac{p^2z^2}{1+p^3+\cfrac{p^3z^2}{1+p^4+\cfrac{p^4z^2}{1+p^5+\text{etc.}}}}}}}$$

$$\Delta\operatorname{am}x = \sqrt{k'}.(P^2+Q^2),$$

$$P+Qi = \cfrac{1}{1+\cfrac{2pz^2}{1-p^2-\cfrac{(1-p^4)pz^2}{1-p^4+\cfrac{(1-p^4)p^3z^2}{1-p^6-\cfrac{(1-p^8)p^3z^2}{1-p^8+\cfrac{(1-p^8)p^5z^2}{1-p^{10}-\text{etc.}}}}}}}$$

$$\operatorname{tang}\operatorname{am} x = \frac{1}{\sqrt{k'}}\operatorname{tang}\frac{\pi x}{2K}.(R^2+S^2),$$

$$R+Si = \cfrac{1}{1-\cfrac{2z^2}{1-p^2+\cfrac{(1-p^4)z^2}{1-p^4-\cfrac{(1-p^4)p^2z^2}{1-p^6+\cfrac{(1-p^8)p^2z^2}{1-p^8-\cfrac{(1-p^8)p^4z^2}{1-p^{10}+\text{etc.}}}}}}}$$

Il existe un grand nombre d'autres développements nouveaux des fonctions elliptiques, que je réserve pour un autre mémoire, où j'essaierai à les expliquer avec leur principes.

Pour le cas où n est un entier *impair*, ω désignant une racine *primitive* de l'équation $\omega^n = 1$, Mr. *Gaufs* a donné la formule

$$1+\omega^{-1}+\omega^{-3}+\omega^{-6}+\dots+\omega^{-\frac{1}{2}(n(n-1))} = (1-\omega)(1-\omega^3)(1-\omega^5)\dots(1-\omega^{n-2}).$$

En transformant ce produit dans la série suivante

$$1+\frac{1-\omega}{1-\omega^2}+\frac{(1-\omega)(1-\omega^3)}{(1-\omega^2)(1-\omega^4)}+\frac{(1-\omega)(1-\omega^3)(1-\omega^5)}{(1-\omega^2)(1-\omega^4)(1-\omega^6)}+\text{etc.}$$

et en développant celle-ci en fraction continue, je trouve

$$\cfrac{1}{1-\cfrac{1}{1+\omega-\cfrac{\omega}{1+\omega^2-\cfrac{\omega^2}{1+\omega^3-\dots-\cfrac{\omega^{n-2}}{1+\omega^{n-1}}}}}}.$$

Cela fournit cette équation remarquable:

$$1+\omega^{-1}+\omega^{-3}+\omega^{-6}+\dots+\omega^{-\frac{1}{2}(n(n-1))}$$
$$= \cfrac{1}{1-\cfrac{1}{1+\omega-\cfrac{\omega}{1+\omega^2-\cfrac{\omega^2}{1+\omega^3-\dots-\cfrac{\omega^{n-2}}{1+\omega^{n-1}}}}}}.$$

D'un autre côté on a, comme l'on sait,

$$1+\omega^{-1}+\omega^{-3}+\omega^{-6}+\dots+\omega^{-\frac{1}{2}(n(n-1))} = \omega^{-\frac{1}{8}(n^2-1)}\sqrt{((-1)^{\frac{1}{2}(n-1)}.n)},$$

où le signe du radical peut être déterminé par les méthodes connues. On a donc aussi

$$\sqrt{((-1)^{\frac{1}{2}(n-1)}.n)} = \cfrac{\omega^{\frac{1}{8}(n^2-1)}}{1-\cfrac{1}{1+\omega-\cfrac{\omega}{1+\omega^2-\cfrac{\omega^2}{1+\omega^3-\cdots-\cfrac{\omega^{n-2}}{1+\omega^{n-1}}}}}}.$$

Cette expression en fraction continue et finie du radical $\sqrt{(\pm n)}$, suivant une loi si simple, me parait très remarquable, et je ne crois pas qu'une formule semblable soit déjà connue.

Je remarque encore que l'on a

$$\left(1-\frac{z}{p}\right)\left(1-\frac{z}{p^2}\right)\left(1-\frac{z}{p^3}\right) \text{ in inf.} = \varphi(z)$$

$$= 1+\cfrac{z}{1-p-\cfrac{z}{\frac{1-p^2}{1-p}+\cfrac{p^2 z}{1-p^3-\cfrac{pz}{\frac{1-p^4}{1-p^2}+\cfrac{p^4 z}{1-p^5-\cfrac{p^2 z}{\frac{1-p^6}{1-p^3}+\text{etc.}}}}}}}$$

Tous les dénominateurs sont ici des fonctions entières de p. Soit $z=1$ et p un nombre entier, tous les dénominateurs et tout les numérateurs seront des nombres entiers, et les premiers surpasseront toujours les derniers. On conclut de là que la valeur du produit infini $\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^3}\right)\dots$ est toujours une quantité *irrationnelle*, p étant entier et >1. A l'aide de la formule $\varphi(z)=\left(1-\frac{z}{p}\right)\varphi\left(\frac{z}{p}\right)$ on peut exprimer rationnellement $\varphi(z)$ par une autre fonction $\varphi(\zeta)$, dont la variable est d'une petitesse arbitraire. En considérant donc attentivement la fraction continue, il sera facile d'en tirer une proposition plus générale; ce que nous laissons au lecteur.

Toutes les fractions continues que nous avons presentées ici, ne sont que des exemples particuliers. Les méthodes que nous avons employées pour y parvenir nous ont fournis des fractions continues d'une généralité telle, que j'ose assurer qu'elles renferment, outre une foule de résultats nouveaux et très rémarquables comme cas spéciaux, toutes les fractions continues trouvées jusqu'à

présent, et surtout toutes celles de Mr. *Gaufs*. C'est ce que nous expliquerons dans une autre occasion.

Ce qui m'a fort intéressé dans ces recherches, ce sont les équations identiques qui se présentent en comparant les résultats. Ainsi, par exemple, parceque la fraction continue dans laquelle nous avous développé la série $1+\omega^{-1}+\omega^{-3}+\ldots$ $\ldots+\omega^{\frac{1}{2}(n(n-1))}$ se trouve aussi sans le secours de la transformation de Mr. *Gaufs*, il en résulte une nouvelle manière de vérifier cette ingénieuse transformation. Il existe des résultats analogues pour les formules qui se rapportent aux fonctions elliptiques.

6.

La loi de réciprocité tireé des formules de Mr. Gauss, sans avoir déterminé préalablement le signe du radical.

(Par Mr. *G. Eisenstein* à Berlin.)

Mr. *Gauss* a déduit la loi de réciprocité entre deux nombres premiers impairs quelconques, des formules remarquables présentées dans son beau mémoire ayant pour titre: „Summatio quarundam serierum singularium." Cette démonstration, qu'on trouve aussi dans un excellent mémoire de Mr. *Dirichlet* *), est maintenant bien connue, et l'on sait que les considérations de Mr. *Gauss* exigent nécessairement *la détermination du signe du radical* qui entre dans les formules citées. Mais la détermination de ce signe est un des problèmes les plus difficiles de la science des nombres, et les recherches préliminaires qu'il y a à faire pour vaincre cette difficulté paraissent diminuer beaucoup la simplicité de cette démonstration. Nous ferons voir ici, comment on peut déduire des formules de Mr. *Gauss*, la loi de réciprocité, *sans avoir déterminé le signe du radical*.

Soient p et q deux nombres premiers impairs, et supposons $q > p$; soit de plus r une racine imaginaire de l'équation $x^p = 1$, et posons pour abréger,

$$\sum_{k=1}^{k=p-1}\left(\frac{k}{p}\right)r^k = S, \quad \sum_{k=1}^{k=p-1}\left(\frac{k}{p}\right)r^{qk} = S_q.$$

Les formules de Mr. *Gauss* donnent les deux équations suivantes:

$$(\alpha.) \quad S_q = \left(\frac{q}{p}\right)S,$$

$$(\beta.) \quad S^2 = (-1)^{\frac{1}{2}(p-1)}p.$$

Si l'on élève la seconde de ces deux équations à la puissance $\frac{1}{2}(q+1)$ et que l'on en rentranche la première après l'avoir multipliée par S, on trouve

$$S^{q+1} - SS_p = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q+1)}p^{\frac{1}{2}(q+1)} - \left(\frac{q}{p}\right)S^2.$$

Substituant la valeur du quarré S^2 fournie par l'equation $(\beta.)$, on aura

*) „Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies. Tome XVII. de ce journal.

$$(\gamma.)\qquad S(S^q - S_q) = (-1)^{\frac{1}{2}(p-1)}p\left((-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right)\right).$$

Pour abreger, nous désignerons l'expression à gauche par χ.

En développant la puissance S^q, on voit aisément qu'elle renferme: 1) Les $q$ièmes puissances de tous les termes individuels de la série S, c'est à dire les termes de la forme $\left(\frac{k}{p}\right)^q r^{qk} = \left(\frac{k}{p}\right) r^{qk}$. La somme de ces termes sera $= S_q$. 2) Un nombre de termes dont les coëfficients sont divisibles par q.

On voit donc que l'expression $S(S^q - S_q)$ peut prendre la forme

$$q(A + Br + Cr^2 + \ldots + Kr^{p-2}),$$

où A, B, C, ... K sont des entiers réels. Donc on a

$$\chi = q(A + Br + Cr^2 + \ldots + Kr^{p-2}).$$

Comme rien n'empêche de remplacer dans tous ces résultats r par ses autres valeurs

$$r^2,\ r^3,\ r^4,\ \ldots\ r^{p-1},$$

on aura aussi

$$\chi = q(A + Br^2 + Cr^4 + \ldots),$$
$$\chi = q(A + Br^3 + Cr^6 + \ldots),$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$
$$\chi = p(A + Br^{p-1} + Cr^{2(p-1)} + \ldots).$$

La somme de ces $p-1$ équations est

$$(p-1)\chi = q((p-1)A - B - C - \ldots - K),$$

ce qui prouve que $(p-1)\chi$ est divisible par q. De là, $p(p-1)$ n'étant pas divisible par q, on conclut

$$(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}p^{\frac{1}{2}(q-1)} \equiv \left(\frac{q}{p}\right) \pmod{q},$$

$$p^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}\left(\frac{q}{p}\right) \pmod{q},$$

d'où l'on tire

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}\left(\frac{q}{p}\right),$$

ce qu'il s'agissait de prouver.

Nous démontrerons par une analyse semblable le théorème rélatif au nombre 2: c'est à dire la formule $\left(\frac{2}{q}\right) = (-1)^{\frac{1}{8}(q^2-1)}$.

En combinant les deux équations suivantes

$$(\Sigma(-1)^{\frac{1}{8}(z^2-1)}z)^2 = 8,\qquad \Sigma(-1)^{\frac{1}{8}(z^2-1)}z^q = (-1)^{\frac{1}{8}(q^2-1)}\Sigma(-1)^{\frac{1}{8}(z^2-1)}z,$$

où ζ désigne une racine primitive de l'équation $x^8 = 1$, et où les sommations doivent s'étendre aux quatre entiers γ inférieurs et premiers à 8, on obtient facilement

$$(\Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^\gamma)[(\Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^\gamma)^q - \Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^{q\gamma}]$$
$$= 8(8^{\frac{1}{2}(q-1)} - (-1)^{\frac{1}{8}(q^2-1)}).$$

On tire de là par les mêmes considérations comme ci-dessus, que le second membre est divisible par q, ce qui donne la congruence

$$8^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{8}(q^2-1)} \pmod{q},$$

donc

$$\left(\frac{8}{q}\right) = \left(\frac{2}{q}\right) = (-1)^{\frac{1}{8}(q^2-1)}.$$

Berlin, Mai 1844.

7.

Neuer Beweis und Verallgemeinerung des Binomischen Lehrsatzes.

(Von Herrn Stud. G. *Eisenstein* zu Berlin.)

Hülfssatz. „Wenn m und n zwei ganze positive Zahlen sind, so geht der Ausdruck

$$\frac{p^m-1}{p^n-1}$$

für $p=1$ in $\frac{m}{n}$ über."

In der That: dividirt man Zähler und Nenner dieses Ausdrucks durch $p-1$, so erhält man

$$\frac{p^{m-1}+p^{m-2}+\dots+p+1}{p^{n-1}+p^{n-2}+\dots+p+1},$$

und dieser Quotient geht offenbar in $\frac{m}{n}$ über für $p=1$. Dasselbe ergiebt sich hieraus leicht, wenn m und n beliebig sind.

Man betrachte den Ausdruck

$$1.\quad \varphi(x,c) = (1+x)(1+px)(1+p^2x)\dots(1+p^{c-1}x).$$

Derselbe genügt offenbar der Relation

$$2.\quad (1+p^cx)\varphi(x) = (1+x)\varphi(px).$$

Da $\varphi(x,c)$ eine ganze Function $c$ten Grades von x ist, so kann man

$$3.\quad \varphi(x,c) = A_0+A_1x+A_2x^2+\dots+A_cx^c$$

setzen, und es handelt sich darum, die Coëfficienten A zu bestimmen. Zunächst ist $A_0=1$. Setzt man, um allgemein A_k zu bestimmen, die Reihen für $\varphi(x)$ und $\varphi(px)$ in die Relation (2.), so erhält man

$$(1+p^cx)\sum_{k=0}^{k=c}A_kx^k = (1+x)\sum_{k=0}^{k=c}A_kp^kx^k;$$

folglich ergiebt sich durch Vergleichung der Glieder, welche auf beiden Seiten in dieselbe Potenz von x multiplicirt sind, die Coëfficientengleichung

$$A_k+p^cA_{k-1} = A_kp^k+A_{k-1}p^{k-1},$$

und hieraus

$$4.\quad A_k = \frac{p^c-p^{k-1}}{p^k-1}A_{k-1},$$

mithin

$$A_k = \frac{p^c-p^{k-1}}{p^k-1}\cdot\frac{p^c-p^{k-2}}{p^{k-1}-1}\dots\frac{p^c-1}{p-1}A_0.$$

Erwägt man, dafs $A_0 = 1$ und $1+2+3+\ldots+t-1 = \frac{1}{2}t(t-1)$ ist, so kann man den Ausdruck für A_t auch wie folgt schreiben:

$$5.\quad A_t = \frac{p^\alpha-1}{p-1}\cdot\frac{p^{\alpha-1}-1}{p^2-1}\cdots\frac{p^{\alpha-t+1}-1}{p^t-1}\cdot p^{\frac{1}{2}t(t-1)}.$$

Man erhält also

$$6.\quad \varphi(x,\alpha) = (1+x)(1+px)(1+p^2x)\ldots(1+p^{\alpha-1}x)$$
$$= \sum_{t=0}^{t=\alpha} A_t x^t = \sum_{t=0}^{t=\alpha}\frac{p^\alpha-1}{p-1}\cdot\frac{p^{\alpha-1}-1}{p^2-1}\cdots\frac{p^{\alpha-t+1}-1}{p^t-1}p^{\frac{1}{2}t(t-1)}x^t.$$

Setzt man in dieser Formel, welche für jeden Werth von p gilt, $p=1$, so kommt links $(1+x)^\alpha$, während rechts der allgemeine Coëfficient A_t nach obigem *Hülfssatze* in

$$\frac{\alpha}{1}\cdot\frac{\alpha-1}{2}\cdot\frac{\alpha-2}{3}\cdots\frac{\alpha-t+1}{t}$$

übergeht, so dafs

$$7.\quad (1+x)^\alpha = 1+\frac{\alpha}{1}x+\frac{\alpha(\alpha-1)}{1.2}x^2+\ldots+x^\alpha \text{ ist.}$$

Man sieht an diesem Beispiele, wie zweckmäfsig es ist, Ausdrücke als *specielle Fälle* von andern, *allgemeineren* zu betrachten. Durch die Einführung der neuen Variabeln p war es möglich, eine Relation von der Form (2.) aufzustellen, die zwar für den speciellen Fall $p=1$ ebenfalls gültig bleibt, aber dann für die Entwicklung nichts liefert, weil sie identisch wird.

Die Coëfficienten A_t, welche im Grunde wieder Functionen von der Form $\varphi(x)$ sind, besitzen ganz ähnliche Eigenschaften wie die Binomialcoëfficienten, und enthalten diese letzteren, wie man sieht, als specielle Fälle in sich. Wenn α und β irgend zwei ganze positive Zahlen sind, und man setzt in der Relation

$$(1+x)(1+px)\ldots(1+p^{\alpha+\beta-1}x) =$$
$$(1+x)(1+px)\ldots(1+p^{\alpha-1}x)\times(1+p^\alpha x)(1+p.p^\alpha x)\ldots(1+p^{\beta-1}.p^\alpha x),$$

d. h. in

$$\varphi(x,\alpha+\beta) = \varphi(x,\alpha).\varphi(p^\alpha x,\beta)$$

die Reihen für die drei Functionen φ aus (6.), und vergleicht dann die entsprechenden Glieder, so erhält man

$$8.\quad C_t = A_t + A_{t-1}B_1p^\alpha + A_{t-2}B_2p^{2\alpha} + \ldots + B_tp^{t\alpha}.$$

Es bedeuten hier B_t, C_t resp. Dasjenige, was aus A_t wird, wenn man β, $\alpha+\beta$ statt α setzt. Stezt man in (8.) überall $p^\alpha = u$, $p^\beta = v$, so gehen beide Seiten in ganze Functionen von u und v über, und es erscheint nirgends α und β

mehr, außer implicite in u und v. Bringt man nun die Gleichung auf Null, so hat man eine *ganze* Function von u und v, die für *unendlich viele* Werthe dieser beiden Variabeln (welche allen ganzen positven Werthen von α und β entsprechen) *verschwindet*, und die also eben deshalb auch nothwendig *identisch* verschwinden muſs, d. h. für jeden Werth von u und v *). Es ist hierdurch die Gültigkeit der Formel (8.) für jeden Werth von α und β bewiesen. Verallgemeinert man nun die Bedeutung von $\varphi(x,\alpha)$, indem man unter diesem Zeichen für jeden Werth von α die Reihe $\sum_{t=0}^{t=\infty} A_t x^t$ versteht (so oft dieselbe convergirt), so folgt aus dem eben Bewiesenen rückwärts, daſs die Relation

$$9. \quad \varphi(x,\alpha+\beta) = \varphi(x,\alpha).\varphi(p^\alpha x,\beta)$$

nicht bloſs für ganze, sondern auch für beliebige Werthe von α und β stattfinde; und hieraus folgt wiederum, wenn man $p=1$ setzt, daſs die Reihe

$$1+\frac{\alpha}{1}x+\frac{\alpha(\alpha-1)}{1.2}x^2+\frac{\alpha(\alpha-1)(\alpha-2)}{1.2.3}x^3 \text{ etc.} = \psi(\alpha)$$

für jeden Werth von α und β der Relation

$$10. \quad \psi(\alpha+\beta) = \psi(\alpha)\psi(\beta)$$

genügt. Diese Relation liefert sogleich mittels bekannter Schlüsse (deren sich z. B. *Dirichlet* und *Ohm* bedienen) den Beweis des *allgemeinen Binomischen Satzes* für *beliebige* Exponenten.

Die Function $\varphi(x,\alpha)$, wie sie in (1.) definirt wurde, ist nur ein specieller Fall des unendlichen Products

$$\frac{(1+x)(1+px)(1+p^2x)\text{ in inf.}}{(1+p^\alpha x)(1+p^{\alpha+1}x)(1+p^{\alpha+2}x)\text{ in inf.}},$$

welches in das dortige $\varphi(x,\alpha)$ übergeht, so oft α eine *positive ganze* Zahl ist. Dieses unendliche Product convergirt immer, wenn man $(p)<1$ annimmt; was wir demnach hier thun wollen. Sucht man dasselbe nach dem obigen Princip in eine Reihe nach Potenzen von x zu entwickeln, so findet man genau dieselbe Entwicklung wie für $\varphi(x,\alpha)$, nur daſs hier α beliebig ist, und es ist für jeden Werth von α:

$$11. \quad \frac{(1+x)(1+px)(1+p^2x)\text{ in inf.}}{(1+p^\alpha x)(1+p^{\alpha+1}x)(1+p^{\alpha+2}x)\text{ in inf.}} = \varphi(x,\alpha) = \sum_{t=0}^{t=\infty} A_t x^t,$$

wo

$$A_t = \frac{(p^\alpha-1)(p^\alpha-p)(p^\alpha-p^2)\dots(p^\alpha-p^{t-1})}{(p-1)(p^2-1)(p^3-1)\dots(p^t-1)}; \quad \text{Mod}(p)<1.$$

---

*) Eine ganze Function muſs schon identisch verschwinden, wenn man nur weiſs, daſs die Anzahl der Werthe der Variabeln, für welche sie verschwindet, ihren Grad um eine Einheit übertrifft.

In dieser Formel ist zugleich ein neuer Beleg für die Richtigkeit der Relation (9.) enthalten.

Die Relation (9.) liefert für specielle Werthe von α und β interessante Resultate. Man sieht z. B., dafs der Quotient der Einheit durch eine Reihe von der Form $\Sigma A_t x^t$ wieder eine Reihe von ähnlicher Form ist, u. s. w.

Setzt man in (11.) $\alpha = \infty$, so wird $p^\alpha = 0$ und man erhält

$$12. \quad (1+x)(1+px)(1+p^2x) \text{ in inf.} = \sum_{t=0}^{t=\infty} \frac{(-1)^t p^{\frac{1}{2}t(t-1)}}{(p-1)(p^2-1)\dots(p^t-1)} x^t.$$

Die unendliche Reihe zur Rechten gehört zu den wenigen, welche *für alle Werthe von x convergiren.* In der That: der Quotient zweier aufeinanderfolgenden Coëfficienten ist

$$-\frac{p^t}{p^{t+1}-1},$$

welches, wegen $N(p) < 1$, gegen Null convergirt für $t = \infty$.

Setzt man in (8.) $p = 1$, so erhält man die Relation zwischen den Binomialcoëfficienten, welche auch unter dem Namen des *Binomischen Satzes für Factoriellen* bekannt ist.

Das Product zur Linken in (12.) verschwindet offenbar für die folgenden Werthe von x:

$$x = -1, \quad -\frac{1}{p}, \quad -\frac{1}{p^2}, \quad -\frac{1}{p^3}, \text{ etc.},$$

und für keine andern; also giebt dies alle Wurzeln der transcendenten Gleichung

$$\sum_{t=0}^{t=\infty} \frac{(-1)^t p^{\frac{1}{2}t(t-1)}}{(p-1)(p^2-1)\dots(p^t-1)} x^t = 0.$$

Diese Bemerkung liefert eine unendliche Anzahl von Reihen, welche alle $= 0$ sind, z. B.

$$1 + \frac{1}{p-1} + \frac{p}{(p-1)(p^2-1)} + \frac{p^3}{(p-1)(p^2-1)(p^3-1)} + \text{ in inf.} = 0,$$

$$1 + \frac{1}{p-1} \cdot \frac{1}{p} + \frac{p}{(p-1)(p^2-1)} \cdot \frac{1}{p^2} + \frac{p^3}{(p-1)(p^2-1)(p^3-1)} \cdot \frac{1}{p^3} + \text{ in inf.} = 0,$$

u. s. w., allgemein

$$\sum_{t=0}^{t=\infty} \frac{p^{\frac{1}{2}t(t-1)}}{(p-1)(p^2-1)\dots(p^t-1)} \cdot \frac{1}{p^{mt}} = 0,$$

für jeden *ganzen positiven* Werth von m. Da diese Reihen für jeden Werth von p verschwinden, so mufs auch, wenn man sie nach aufsteigenden Potenzen p mit constanten Coëfficienten entwickelt, jeder einzelne Coëfficient verschwinden. Dies giebt eine Reihe ziemlich interessanter Sätze. Z. B. die

erste Reihe liefert, wegen

$$\frac{1}{1-p} = \sum_{s=0}^{s=\infty} p^s, \quad \frac{1}{1-p^2} = \sum_{s=0}^{s=\infty} p^{2s}, \text{ etc.},$$

$$1 - \Sigma p^{s_1} + p\,\Sigma p^{s_1+2s_2} - p^3\,\Sigma p^{s_1+2s_2+3s_3} + \ldots + (-1)^t p^{\frac{1}{2}t(t-1)}\,\Sigma p^{s_1+2s_2+\ldots+ts_t}$$
$$+ \text{ in inf.} = 0,$$

wo jede der Zahlen s_1, s_2, ... alle Werthe von 0 bis ∞ durchläuft. Bezeichnet man durch $f(k, t)$ die Anzahl der Lösungen der Gleichung

$$k = s_1 + 2s_2 + 3s_3 + \ldots + ts_t,$$

so ist der Coëfficient von p^k offenbar

$$= -f(k, 1) + f(k-1, 2) - f(k-3, 3) + f(k-6, 4) - \ldots$$
$$\ldots + (-1)^t f(k - \tfrac{1}{2}t(t-1), t) + \text{ etc.},$$

also ist

$$0 = f(k, 1) - f(k-1, 2) + f(k-3, 3) - f(k-6, 4) + \text{ etc.},$$

bis die Reihe von selbst abbricht.

Allgemein erhält man auf dieselbe Weise:

$$f(k+m, 1) - f(k+2m-1, 2) + f(k+3m-3, 3) - f(k+4m-6, 4) + \text{ etc.} = 0.$$

Ähnliche Folgerungen lassen sich an die allgemeineren Formeln (11.) knüpfen.

Berlin, im Mai 1844.

8.

Entwicklung von $\alpha^{\alpha^{\alpha^{\cdot^{\cdot^{\cdot}}}}}$.

(Von Hrn. Stud. G. *Eisenstein* zu Berlin.)

Wenn α positiv und < 1 ist, so folgt aus

$$\alpha^{\alpha^{\alpha \text{ in inf.}}} = \beta:$$

$$\alpha^{\beta} = \beta,$$

folglich ist β aus der transcendenten Gleichung

$$\sqrt[\beta]{\beta} = \alpha$$

zu bestimmen. Statt dieser betrachte man die allgemeinere Gleichung

$$(1.) \qquad x^{x^n} = y.$$

Setzt man $x = e^{\xi}$, $y = e^{\eta}$, welches $\xi = \log x$, $\eta = \log y$ giebt, so geht die Gleichung (1.) in

$$(2.) \qquad \xi e^{n\xi} = \eta$$

über. Um ξ, oder allgemeiner ξ^m in η auszudrücken, wollen wir

$$(3.) \qquad \xi^m = \eta^m \sum_{t=\infty}^{t=0} A_t \eta^t$$

setzen und die Coëfficienten A_t zu bestimmen suchen. Differenziirt man die Gleichung (3.) auf beiden Seiten nach ξ, so kommt

$$m\xi^{m-1} = \Sigma(t+m) A_t \eta^{t+m-1} . \frac{\partial \eta}{\partial \xi}.$$

Es sei p eine positive ganze Zahl (oder Null), und man multiplicire die letztere Gleichung auf beiden Seiten mit $\eta^{-(m+p)}$, so dafs

$$(4.) \qquad m\xi^{m-1}\eta^{-(m+p)} = \sum_{t=0}^{t=\infty} (t+m) A_t \eta^{t-p-1} . \frac{\partial \eta}{\partial \xi}$$

$$= \sum_{t=0}^{t=p-1} \frac{t+m}{t-p} A_t \frac{\partial(\eta^{t-p})}{d\xi} + (p+m) A_p : \frac{\partial(\log \eta)}{\partial \xi} + \sum_{t=p+1}^{t=\infty} \frac{t+m}{t-p} A_t \frac{\partial(\eta^{t-p})}{\partial \xi}.$$

Aus (2.) erhält man

$$\xi^{m-1}\eta^{-(m+p)} = \xi^{-p-1} e^{-(m+p)n\xi} = \sum_{s=\infty}^{s=0} \frac{(-1)^s n^s (m+p)^s}{s!} \xi^{s-p-1};$$

$$\eta^{t-p} = \xi^{t-p} e^{(t-p)n\xi} = \sum_{s=0}^{s=\infty} \frac{n^s (t-p)^s}{s!} \xi^{s+t-p},$$

$$\frac{\partial(\eta^{t-p})}{\partial \xi} = \sum_{s=\infty}^{s=0} (s+t-p) \frac{n^s (t-p)^s}{s!} \xi^{s+t-p-1};$$

und endlich $\log\eta = \log\xi + n\xi$, folglich

$$\frac{\partial(\log\eta)}{\partial\xi} = \xi^{-1} + n.$$

Setzt man alle diese Werthe in die Gleichung (4.), so wird dieselbe nur noch die Variable ξ enthalten, und man erhält

$$(5.)\qquad m\sum_{s=0}^{s=\infty}\frac{(-1)^s n^s (m+p)^s}{s!}\xi^{s-p-1}$$

$$= \sum_{t=0}^{t=\infty}\left(\frac{t+m}{t-p}A_t\sum_{s=0}^{s=\infty}(s+t-p)\frac{n^s(t-p)^s}{s!}\xi^{s+t-p-1}\right) + (p+m)A_p\xi^{-1} + n(p+m)A_p.$$

In der Summe zur Rechten ist der Werth $t=p$ auszuschliefsen. Vergleicht man hier alle diejenigen Glieder, welche auf beiden Seiten mit ξ^{-1} multiplicirt sind, so ergiebt sich

$$m\frac{(-1)^p n^p (m+p)^p}{p!} = (p+m)A_p,$$

also

$$(6.)\qquad A_p = m.\frac{(-1)^p n^p (m+p)^{p-1}}{p!},$$

so dafs

$$(7.)\qquad \xi^m = \eta^m\sum_{t=0}^{t=\infty}\frac{(-1)^t n^t (m+t)^{t-1}}{t!}\eta^t$$

ist. Die Gleichung (5.) liefert noch, nach Einsetzung der Werthe von A_t, durch Vergleichung der übrigen Potenzen von ξ unendlich viele Gleichungen, welche für unsern Zweck nicht nöthig sind.

Aus der Gleichung $\xi e^{n\xi} = \eta$ zieht man $e^{\lambda\xi} = \left(\frac{\eta}{\xi}\right)^{\frac{\lambda}{n}} = \frac{\xi^{-\frac{\lambda}{n}}}{\eta^{-\frac{\lambda}{n}}}$; aber zufolge Gleichung (7.) ist

$$\frac{\xi^{-\frac{\lambda}{n}}}{\eta^{-\frac{\lambda}{n}}} = \sum_{t=0}^{t=\infty}\lambda\frac{(\lambda-nt)^{t-1}}{t!}\eta^t,$$

also ist

$$(8.)\qquad x^\lambda = \lambda\sum_{t=0}^{t=\infty}\frac{(\lambda-nt)^{t-1}}{t!}(\log y)^t$$

für $x^{x^n} = y$.

Diese Reihen sind ziemlich merkwürdig, weil in ihnen die Grundzahlen und Exponenten *zugleich* in arithmetischer Ordnung fortschreiten. Man erhält z. B.

$$x = 1 + \log y - \frac{(\log y)^2}{2!} + 2^2\frac{(\log y)^3}{3!} - 3^3\frac{(\log y)^4}{4!} + \text{etc.},$$

wenn $x^x = y$ ist,

$$x = 1+\log y + 3^1\frac{(\log y)^2}{2!} + 4^2\frac{(\log y)^3}{3!} + 5^3\frac{(\log y)^4}{4!} + \text{etc},$$

wenn $\sqrt[x]{x} = y$ ist, u. s. w. Auch sieht man, dafs das Product beliebig vieler solcher Reihen wieder eine Reihe von derselben Form hervorbringt.

Um die *Convergenz* der Reihen in (8.) zu untersuchen, wollen wir den Quotienten aus dem $t+1$ten durch den $t$ten Coëfficienten betrachten. Dieser Quotient ist

$$= \frac{1}{t+1}\cdot\frac{(\lambda-nt-n)^t}{(\lambda-nt)^{t-1}} = \frac{-n}{1+\frac{1}{t}} \times \frac{\left(1-\frac{\lambda-n}{nt}\right)^t}{\left(1-\frac{\lambda}{nt}\right)^t}.$$

Für $t=\infty$ convergirt der erste Factor gegen $-n$, während Zähler und Nenner des zweiten Factors nach einem bekannten Satze resp. gegen $e^{-\frac{\lambda-n}{n}}$ und $e^{-\frac{\lambda}{n}}$ convergiren, so dafs die Grenze des ganzen Ausdrucks

$$= -n\frac{e^{-\frac{\lambda-n}{n}}}{e^{-\frac{\lambda}{n}}} = -ne$$

für $t=\infty$ ist.

Die Reihe (8.) *convergirt demnach für alle Werthe von* $\log y$, *welche zwischen* $-\frac{1}{ne}$ *und* $+\frac{1}{ne}$ *liegen, also für alle Werthe von y zwischen*

$$\frac{1}{\sqrt[ne]{e}} \text{ und } \sqrt[ne]{e}.\text{“}$$

Dem ersten dieser beiden Grenzwerthe entspricht offenbar der Werth $x=e^{-\frac{1}{n}}$. Es ist merkwürdig, dafs dieser Werth mit demjenigen zusammenfällt, für welchen die Curve, deren Gleichung zwischen rechtwinkligen Coordinaten

$$y = x^{x^n}$$

ist, ein ***Minimum*** oder ***Maximum*** hat, je nachdem n resp. *positiv* oder *negativ* ist. Man sehe die Figuren 1. und 2. (Taf. I.).

Wir hatten aus $\alpha^{\alpha^{\alpha^{\cdot^{\cdot}}}} = \beta$, wenn $\alpha < 1$ ist, $\sqrt[\beta]{\beta} = \alpha$ gefunden, also ergiebt sich jetzt

$$\alpha^{\alpha^{\alpha \text{ in inf.}}} = 1+\log\alpha + 3\frac{(\log\alpha)^2}{2!} + 4^2\frac{(\log\alpha)^3}{3!} + 5^3\frac{(\log\alpha)^4}{4!} + 6^4\frac{(\log\alpha)^5}{5!} + \text{etc.},$$

und dieses Resultat gilt

$$\textit{von } \alpha = \frac{1}{\sqrt[e]{e}} = 0{,}6922 \text{ (excl.) } \textit{bis } \alpha = 1 \text{ (incl.)}.$$

Die hier aufgestellten Reihen waren ein erster mathematischer Versuch in meinem funfzehnten Jahre. Ich berechnete damals auch eine kleine Tafel, welche aus der Gleichung $x^x = y$ für ein gegebenes y das zugehörige x bestimmt. Ich will sie hier dem gegenwärtigen Aufsatze beifügen.

y	x	y	x	y	x	y	x	y	x
1	1,000000	11	2,555605	21	2,879069	31	3,065491	50	3,287261
2	1,559611	12	2,600295	22	2,901638	32	3,080448	60	3,370040
3	1,825456	13	2,641062	23	2,923122	33	3,094912	99	3,592876
4	2,000000	14	2,678524	24	2,943622	34	3,108915	100	3,597285
5	2,129373	15	2,713164	25	2,963220	35	3,122484	101	3,601647
6	2,231829	16	2,745381	26	2,981991	36	3,135642	102	3,605960
7	2,316455	17	2,775449	27	3,000000	37	3,148415	103	3,610241
8	2,388427	18	2,803663	28	3,017306	38	3,160828	104	3,614468
9	2,450954	19	2,830223	29	3,033959	39	3,172894	105	3,618654
10	2,506186	20	2,855309	30	3,050009	40	3,184633		

Die Curven, deren Gleichung $x^{x^n} = y$ ist, dürften für den Anfänger in der analytischen Geometrie ein instructives Übungsbeispiel darbieten.

Berlin, im Mai 1844.

9.

Lois de réciprocité.

(Par Mr. G. *Eisenstein* à Berlin.)

Nouvelle démonstration du théorème fondamental sur les résidus quadratiques dans la théorie des nombres complexes. Démonstration du théorème fondamental sur les résidus biquadratiques. Le théorème le plus général sur les caractères biquadratiques, qui comprend, comme cas particulier, le théorème fondamental.

Soit p un nombre premier réel $4n+1$, soient p_1, p_2 les deux nombres premiers *complexes* de la forme $\alpha+\beta i$ qui, ayant p pour norme commune, sont tels que $p_1 \equiv p_2 \equiv 1$ (mod. 2) et $p_1 p_2 = p$. Soit de plus r une racine de l'équation $\frac{x^p-1}{x-1}=0$, et désignons par le symbole $\left[\frac{k}{p_1}\right]$ la puissance évidemment unique de i qui satisfait la congruence

$$k^{\frac{1}{4}(p-1)} \equiv \left[\frac{k}{p_1}\right] \quad (\text{mod. } p_1).$$

Cela posé, on a comme l'on sait, et comme nous l'avons déjà prouvé,

$$\left(\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right]r^k\right)^4 = S^4 = p(a+bi)^2; \quad (a+bi)(a-bi) = p,$$

$$\left(\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right]^3 r^k\right)^4 = T^4 = p(a-bi)^2; \quad a+bi \equiv a-bi \equiv 1 \ (\text{mod. } 2).$$

Je dis que l'on peut poser $a+bi=p_1$. Nous avons prouvé dans une autre occasion*) que l'on a

$$a+bi = \sum_{\sigma=1}^{\sigma=p-2}\left[\frac{\sigma}{p_1}\right]\left[\frac{\sigma+1}{p_1}\right]^2, \quad a-bi = \sum_{\sigma=1}^{\sigma=p-2}\left[\frac{\sigma}{p_1}\right]^3\left[\frac{\sigma+1}{p_1}\right]^2,$$

ce qui donne

$$a+bi \equiv \sum_{\sigma=1}^{\sigma=p-2}\sigma^{\frac{1}{4}(p-1)}(\sigma+1)^{\frac{1}{2}(p-1)} \quad (\text{mod. } p_1),$$

$$a-bi \equiv \sum_{\sigma=1}^{\sigma=p-2}\sigma^{\frac{3}{4}(p-1)}(\sigma+1)^{\frac{1}{2}(p-1)} \quad (\text{mod. } p_1);$$

mais il a été aussi démontré que ces deux dernières sommes sont respectivement

$$\equiv 0 \ (\text{mod. } p), \quad \equiv -\frac{(\frac{1}{2}(p-1))!}{(\frac{1}{4}(p-1))!\,(\frac{1}{4}(p-1))!} \ (\text{mod. } p):$$

---

*) Voir „Beiträge zur Kreistheilung" cahier 3. vol. 27. de ce journal.

en désignant par $m!$ le produit $1.2.3\ldots.m$. On a donc

$$a+bi \equiv 0 \pmod{p_1}, \qquad a-bi \equiv -\frac{(\frac12(p-1))!}{(\frac14(p-1))!\,(\frac14(p-1))!} \pmod{p_1}.$$

Mais p_2 n'étant pas divisible par p_1, il faut que $a+bi = p_1$. Celà étant, on obtient encore $a-bi = p_2$, parsuite

$$p_2 \equiv -\frac{(\frac12(p-1))!}{(\frac14(p-1))!\,(\frac14(p-1))!} \pmod{p_1},$$

et de même

$$p_1 \equiv -\frac{(\frac12(p-1))!}{(\frac14(p-1))!\,(\frac14(p-1))!} \pmod{p_2},$$

ce que je remarque en passant.

Dans ce qui suit nous ferons surtout usage de ces deux équations:

$$(1.)\quad \Big(\sum_{k=1}^{k=p-1}\Big[\frac{k}{p_1}\Big]r^k\Big)^4 = S^4 = pp_1^2,$$

$$(2.)\quad \Big(\sum_{k=1}^{k=p-1}\Big[\frac{k}{p_1}\Big]^3 r^k\Big)^4 = T^4 = pp_2^2.$$

Soit q un nombre premier *réel* de la forme $4n+3$. En élevant les deux membres de l'équation (1.) à la puissance $\frac14(q^2+3)$ il vient

$$(3.)\quad S^{q^2+3} = (pp_1^2)^{\frac14(q^2+3)}.$$

D'un autre côté, on a aussi, comme l'on sait,

$$(4.)\quad \sum_{k=1}^{k=p-1}\Big[\frac{k}{p_1}\Big]r^{q^2k} = S_{q^2} = \Big[\frac{q^2}{p_1}\Big].S.$$

En combinant cette équation, après l'avoir multipliée par S^3, avec l'équation (1.) on en tire

$$(5.)\quad S^4 S_{q^2} = \Big[\frac{q^2}{p_1}\Big]pp_1^2.$$

Retranchant l'équation (5.) de celle (3.) il vient

$$(6.)\quad S^4\{S^{q^2-1}-S_{q^2}\} = pp_1^2\Big\{(pp_1^2)^{\frac14(q^2-1)}-\Big[\frac{q^2}{p_1}\Big]\Big\}.$$

Il est aisé de voir que le premier membre de cette dernière équation peut prendre la forme

$$q(A+Br+Cr^2+\ldots.)$$

où $A, B, C, \ldots.$ sont des entiers complexes. On a donc

$$(7.)\quad pp_1^2\Big\{(pp_1^2)^{\frac14(q^2-1)}-\Big[\frac{q^2}{p_1}\Big]\Big\} = q(A+Br+Cr^2+\ldots.).$$

Comme cette équation subsiste quel que soit la valeur de la racine r, elle prouve que l'entier complexe qui compose le premier membre est divisible par q. Si l'on remarque encore que pp_1^2 n'est pas divisible par le nombre premier q, on a la congruence

$$(8.)\quad (pp_1^2)^{\frac{1}{4}(q^2-1)} \equiv \left[\frac{q^2}{p_1}\right] \quad (\text{mod. } q),$$

et cela donne, q^2 étant la norme de q,

$$\left[\frac{pp_1^2}{q}\right] = \left[\frac{q^2}{p_1}\right].$$

Puisque évidemment $\left[\frac{p}{q}\right] = 1$, il vient

$$(9.)\quad \left[\frac{p_1}{q}\right]^2 = \left[\frac{q}{p_1}\right]^2.$$

Mais $\left[\frac{p_1}{q}\right]^2 = 1$, ou $= -1$, selon que p_1 est résidu ou non-résidu quadratique de q (dans la théorie de nombres complexes), et $\left[\frac{q}{p_1}\right]^2 = +1$, ou $= -1$, selon que q est résidu ou non-residu quadratique de p_1; et comme l'expression $\left[\frac{p_1}{q}\right]^2$ ne change pas de valeur en remplaçant p_1 par $-p_1$, l'équation que nous venons de trouver donne le théorème suivant:

Théorème I. *„Etant donnés deux nombres premiers complexes qui sont respectivement de première et de seconde espèce, et dont les parties réelles sont impaires, le premier est ou n'est pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier.*

Soit maintenant h un autre nombre premier réel de la forme $4n+1$, différent de p, et soient h_1, h_2 (que l'on suppose $\equiv 1$ (mod. 2)) les deux nombres premiers complexes conjugués qui ont h pour norme commune. En élévant les deux membres de l'équation (1.) à la puissance $\frac{1}{4}(h+3)$, on aura

$$(10.)\quad S^{h+3} = (pp_1^2)^{\frac{1}{4}(h+3)}.$$

D'un autre côté on a

$$(11.)\quad \sum_{k=1}^{k=p-1} \left[\frac{k}{p_1}\right] r^{hk} = S_h = \left[\frac{h}{p_1}\right]^3 S.$$

Multipliant par S^3 et substituant la valeur de S^4 donnée par (1.), il viendra

$$(12.)\quad S^3 S_h = \left[\frac{h}{p_1}\right]^3 pp_1^2.$$

Enfin les deux équations (10.) et (12.) donnent, en les retranchant l'une de l'autre:

$$(13.)\quad S^3\{S^h - S_h\} = pp_1^2\left\{(pp_1^2)^{\frac{1}{4}(h-1)} - \left[\frac{h}{p_1}\right]^3\right\}.$$

Le premier membre de cette équation étant développé, peut prendre la forme

$$h(A+Br+Cr^2+\ldots.),$$

où A, B, C, ... sont des *entiers* complexes; de sorte que l'on a

$$(14.)\quad pp_1^2\left\{(pp_1^2)^{\frac{1}{4}(k-1)}-\left[\frac{k}{p_1}\right]^3\right\}=k(A+Br+Cr^2+\dots).$$

Comme cette équation subsiste quel que soit la racine r, on en peut conclure que le premier membre est divisible par k, et cela, pp_1^2 n'ayant pas de facteur commun avec k, donne:

$$(15.)\quad (pp_1^2)^{\frac{1}{4}(k-1)}\equiv\left[\frac{k}{p_1}\right]^3\ (\text{mod. } k).$$

On a donc à plus forte raison

$$(16.)\quad (pp_1^2)^{\frac{1}{4}(k-1)}\equiv\left[\frac{k}{p_1}\right]^3\ (\text{mod. } k_1),$$

d'où l'on tire, k étant la norme de k_1,

$$(17.)\quad \left[\frac{pp_1^2}{k_1}\right]=\left[\frac{k^3}{p_1}\right].$$

De même, en échangeant entre eux les nombres premiers réels p et k de la forme $4n+1$, on a

$$(18.)\quad \left[\frac{kk_1^2}{p_1}\right]=\left[\frac{p^3}{k_1}\right].$$

Donc

$$\left[\frac{pp_1^2}{k_1}\right]=\left[\frac{k^3}{p_1}\right]\quad\text{et}\quad\left[\frac{p^3}{k_1}\right]=\left[\frac{kk_1^2}{p_1}\right],$$

ce qui donne, en multipliant,

$$\left[\frac{p^4p_1^2}{k_1}\right]=\left[\frac{k^4k_1^2}{p_1}\right].$$

$$\text{Or }\left[\frac{p^4}{k_1}\right]=\left[\frac{k^4}{p_1}\right]=1,\ \text{donc}$$

$$(19.)\quad \left[\frac{p_1}{k_1}\right]^2=\left[\frac{k_1}{p_1}\right]^2.$$

Cette équation fournit le théorème suivant:

Théorème II. „*Des deux nombres premiers complexes de seconde espèce, dont les parties réelles sont impaires, le premier est ou n'est pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier.*"

Si les nombres premiers q et q' sont tous deux de première espèce, c'est à dire $\equiv 3$ (mod. 4), on a suivant le théorème de *Fermat* $q'^{\frac{1}{4}(q^2-1)}=(q'^{\frac{1}{4}(q+1)})^{q-1}\equiv 1$ (mod. q), donc on a nécessairement $\left[\frac{q'}{q}\right]=1$, et de même $\left[\frac{q}{q'}\right]=1$, et aussi dans ce cas $\left[\frac{q'}{q}\right]=\left[\frac{q}{q'}\right]$, et $\left[\frac{q'}{q}\right]^2=\left[\frac{q}{q'}\right]^2$. A l'aide de cette re-

marque nous pouvons réunir dans l'énoncé suivant les deux théorèmes que nous venons de trouver.

Théorème III. „*Désignant par $\alpha+\beta i$, $\gamma+\delta i$ (β et δ étant pairs et réduisible à zéro) deux nombres premiers complexes quelconques, le premier est ou n'est pas résidu quadratique du second selon que le second est ou n'est pas résidu quadratique du premier.*"

Ce théorème remarquable qui embrasse presque tout ce qu'il y a à dire sur la théorie des résidus quadratiques est redevable à Mr. *Gauss*. Il a été démontré pour la première fois par Mr. *Dirichlet* dans le 9[ième] vol. de ce journal. La démonstration que donne ce grand géomètre est fondé sur le théorème analogue dans la théorie réelle, généralement connu sous le nom „Loi de réciprocité de *Legendre*," tandis que la nôtre est entièrement indépendante de cet autre théorème.

Passons aux résidus *biquadratiques*. Toutes les lettres ayant la même signification comme dans ce qui précède, si l'on élève l'équation (1.) à la puissance $\frac{1}{8}(q^2-1)$, on obtient

$$(20.)\qquad S^{\frac{1}{4}(p^2-1)} = p^{\frac{1}{8}(q^2-1)}p_1^{\frac{1}{8}(q^2-1)}.$$

La puissance $S^{\frac{1}{4}(q^2-1)}$ peut s'écrire $(S^{q+1})^{\frac{1}{4}(q-1)}$. L'expression S^q étant développée suivant le théorème polynomial, peut prendre la forme

$$q(A+Br+Cr^2+\ldots.)+\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right]^q r^{qk},$$

où A, B, C, ... sont des entiers complexes. Or $q\equiv 3$ (mod. 4), donc

$$\left[\frac{k}{p_1}\right]^q = \left[\frac{k}{p_1}\right]^3,\quad \text{et partant}\quad \Sigma\left[\frac{k}{p_1}\right]^q r^{qk} = \Sigma\left[\frac{k}{p_1}\right]^3 r^{qk} = \left[\frac{q}{p_1}\right]T.$$

Substituant, il vient

$$S^q = q(A+Br+Cr^2+\ldots.)+\left[\frac{q}{p_1}\right]T.$$

Multipliant par S et élévant à la puissance $\frac{1}{4}(q-1)$, on a

$$\begin{aligned} S^{\frac{1}{4}(q^2-1)} &= S^{\frac{1}{4}(q-1)}\left\{q(A'+B'r+C'r^2+\ldots.)+\left[\frac{q}{p_1}\right]^{\frac{1}{4}(q-1)}T^{\frac{1}{4}(q-1)}\right\}\\ &= q(A''+B''r+C''r^2+\ldots.)+\left[\frac{q}{p_1}\right]^{\frac{1}{4}(q-1)}(ST)^{\frac{1}{4}(q-1)}\\ &= q(A''+B''r+C''r^2+\ldots.)+\left[\frac{q}{p_1}\right]^{\frac{1}{4}(q-1)}p^{\frac{1}{4}(q-1)}(-1)^{\frac{1}{4}(p-1)\frac{1}{4}(q-1)}, \end{aligned}$$

où A' etc. A'' etc. sont également des entiers complexes. Il suit de là et

de l'équation (20.), que la différence

$$p^{\frac{1}{4}(q^2-1)} p_1^{\frac{1}{4}(q^2-1)} - \left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)} (-1)^{\frac{1}{4}(p-1)\frac{1}{2}(q-1)}$$

est *divisible par q*. D'un autre côté, en se servant de la notation de *Legendre*, on a

$$p^{\frac{1}{2}(q-1)} \equiv \left(\frac{p}{q}\right) \text{ (mod. } q),$$

$$p^{\frac{1}{4}(q^2-1)} = (p^{\frac{1}{2}(q-1)})^{\frac{1}{2}(q+1)} \equiv \left(\frac{p}{q}\right)^{\frac{1}{2}(q+1)} \text{ (mod. } q),$$

donc, en remarquant que $\frac{1}{2}(q-1)$ est impair, on a

$$(21.) \quad p_1^{\frac{1}{4}(q^2-1)} \equiv \left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)} \left(\frac{p}{q}\right)^{\frac{1}{4}(q-3)} (-1)^{\frac{1}{4}(p-1)} \text{ (mod. } q).$$

Cette congruence donne l'équation

$$(22.) \quad \left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)} \left(\frac{p}{q}\right)^{\frac{1}{4}(q-3)} (-1)^{\frac{1}{4}(p-1)}.$$

Soit en premier lieu q de la forme $8n+3$, on a $\frac{1}{2}(q-1) \equiv 1$ (mod. 4) $\frac{1}{4}(q-3) = 0$ (mod. 2), donc

$$\left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right](-1)^{\frac{1}{4}(p-1)}, \quad \text{or} \quad (-1)^{\frac{1}{4}(p-1)} = \left[\frac{-1}{p_1}\right], \quad \text{donc} \quad \left[\frac{p_1}{p}\right] = \left[\frac{-q}{p_1}\right].$$

Soit en second lieu q de la forme $8n+7$, on a $\frac{1}{2}(q-1) \equiv 3$ (mod. 4), $\frac{1}{4}(q-3) \equiv 1$ (mod. 2), donc

$$\left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right]^3 \left(\frac{p}{q}\right) \left[\frac{-1}{p_1}\right].$$

Or p étant de la forme $4n+1$, on peut remplacer $\left(\frac{p}{q}\right)$ par $\left(\frac{q}{p}\right)$. Je dis maintenant que l'on a $\left(\frac{q}{p}\right) = \left[\frac{q}{p_1}\right]^2$ En effet, $\left(\frac{q}{p}\right) \equiv (q^2)^{\frac{1}{4}(p-1)}$ (mod. p), donc à plus forte raison $\left(\frac{q}{p}\right) \equiv (q^2)^{\frac{1}{4}(p-1)}$ (mod. p_1), ce qui donne $\left(\frac{q}{p}\right) = \left[\frac{q^2}{p_1}\right] = \left[\frac{q}{p_1}\right]^2$. Substituant cette valeur, il vient

$$\left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right]^5 \left[\frac{-1}{p_1}\right] = \left[\frac{-q}{p_1}\right].$$

Les deux cas que nous venons de distinguer conduisant au même résultat, nous pouvons énoncer le théorème suivant:

Théorème IV. *„Désignant par q un nombre premier réel et positiv $4n+3$, et par p_1 un nombre premier complexe de seconde espèce, dont la partie réelle est impaire, le caractère biquadratique de $-q$ par rapport à p_1 est toujours le même que le caractère biquadratique de p_1 par rapport à q."*

Voilà la première partie du théorème fondamental sur les résidus biquadratiques.

Pour les recherches que nous aurons à exposer encore, il sera convenable de généraliser la signification du symbole $\left[\frac{M}{l}\right]$. Ce symbole, tel que nous l'avons employé jusqu'ici, suppose que l soit un nombre premier complexe impair, M étant un entier complexe quelconque non-divisible par l, et nous avons désigné par là la puissance évidemment unique de i qui satisfait à la congruence

$$M^{\frac{1}{4}(N(l)-1)} \equiv \left[\frac{M}{l}\right] \quad (\text{mod. } l),$$

$N(l)$ étant la norme de l.

Soient $l, l', l'', \ldots.$ des nombres premiers complexes impairs non-diviseurs de M, mais d'ailleurs égaux ou inégaux, et soit $l\,l'\,l''\ldots. = L$, nous désignerons désormais par

$$\left[\frac{M}{L}\right]$$

le produit

$$(23.)\quad \left[\frac{M}{L}\right] = \left[\frac{M}{l}\right]\left[\frac{M}{l'}\right]\left[\frac{M}{l''}\right]\ldots.$$

L'exposant de la puissance de i qui équivaut à $\left[\frac{M}{L}\right]$ sera nommé le *caractère biquadratique* de M par rapport à L.

Par rapport à notre symbole ainsi généralisé, on aura les formules suivantes dont la démonstration se présente d'elle même et dont l'usage est très fréquent:

$$(24.)\quad \left[\frac{M}{L}\right] = \left[\frac{P}{L}\right],\quad \left[\frac{MM'}{L}\right] = \left[\frac{M}{L}\right]\left[\frac{M'}{L}\right],\quad \left[\frac{M}{LL'}\right] = \left[\frac{M}{L}\right]\left[\frac{M}{L'}\right],$$
$$\left[\frac{M}{L}\right]^2 = \pm 1,\quad \left[\frac{M}{L}\right]^4 = 1:$$

équations qui supposent, la première, que M, toujours sans diviseurs commun avec l'entier complexe impair L, est $\equiv P$ (mod. L); la seconde que M et M' sont premiers à M, et la troisième que M est premier aux entiers impairs L et L'.

Lemme I. „$\alpha+\beta i$ et $\gamma+\delta i$ étant deux entiers complexes quelconques sans diviseur commun, on a toujours

$$\left[\frac{\alpha+\beta i}{\gamma+\delta i}\right] = \left[\frac{\alpha-\beta i}{\gamma-\delta i}\right]^3.\text{“} \quad *)$$

---

*) Ici et dans tout ce qui va suivre on suppose tacitement que les dénominateurs des

La vérité du lemme sera évidente, si nous pouvons le vérifier dans les cas particulier où $\gamma+\delta i$ se réduit à un nombre premier. Avec cette restriction on aura

$$\left[\frac{\alpha-\beta i}{\gamma-\delta i}\right] \equiv (\alpha-\beta i)^{\frac{1}{4}(\gamma^2+\delta^2-1)} \ (\text{mod.}\,(\gamma-\delta i)),$$

c'est à dire

$$\left[\frac{\alpha-\beta i}{\gamma-\delta i}\right] = (m+ni)(\gamma-\delta i)+(\alpha-\beta i)^{\frac{1}{4}(\gamma^2+\delta^2-1)} = i^k$$

où m et n sont deux entiers réels. De là, en remplaçant partout i par $-i$, il suit

$$(-i)^k = \left[\frac{\alpha-\beta i}{\gamma-\delta i}\right]^3 \equiv (\alpha+\beta i)^{\frac{1}{4}(\gamma^2+\delta^2-1)} \ (\text{mod.}\,\gamma+\delta i),$$

ce qu'il s'agissait de prouver.

Lemme II. „A et B étant deux entiers ***réels*** et sans diviseur commun, on a toujours $\left[\frac{A}{B}\right] = 1.$"

Soit d'abord q un nombre premier réel de la forme $4n+3$ (abstraction faite du signe), on aura évidemment $\left[\frac{A}{q}\right]=1$, puisque $\left[\frac{A}{q}\right]\equiv(A^{\frac{1}{4}(q+1)})^{q-1}$ $\equiv 1$ (mod. q), en vertu du théorème de ***Fermat***. Soient en second lieu p_1 et p_2 deux nombres premiers conjugués de seconde espèce qui ont p pour norme commune, on a (Lemme I.), A étant réel,

$$\left[\frac{A}{p_1}\right] = \left[\frac{A}{p_2}\right]^3, \quad \text{donc} \quad \left[\frac{A}{p_1}\right]\left[\frac{A}{p_2}\right] = \left[\frac{A}{p}\right] = \left[\frac{A}{p_2}\right]^4 = 1.$$

Si donc on suppose $B=qq'q''\ldots.pp'p''\ldots.$, $q, q', q'', \ldots.$ étant des nombres premiers ***réels*** $4n+3$, $p, p', p'', \ldots.$ des nombres premiers ***réels*** $4n+1$, on a

$$\left[\frac{A}{B}\right] = \left[\frac{A}{q}\right]\left[\frac{A}{q'}\right]\left[\frac{A}{q''}\right]\ldots. \left[\frac{A}{p}\right]\left[\frac{A}{p'}\right]\left[\frac{A}{p''}\right]\ldots. = 1.$$

Lemme III. „Désignant par A un entier ***réel*** qui avec son signe est $\equiv 1$ (mod. 4), et par L un entier complexe quelconque, je dis qu'on a l'équation $\left[\frac{L}{A}\right] = \left[\frac{A}{L}\right]$."

L'entier réel A étant $\equiv 1$ (mod. 4.), il peut être décomposé dans un nombre de facteurs premiers réels q de la forme $4n+3$ pris chacun avec

---

symboles [=] sont impairs et qu'ils n'ont pas de diviseur commun avec les numérateurs. On suppose aussi que tous les entiers complexes impairs sont pris tels, que leur parties réelles soint impaires.

le signe *moins*, et dans un nombre de facteurs premiers réels p de la forme $4n+1$ pris chacun avec le signe *plus*. A l'aide de la seconde et de la troisième des équations (24.) tout se réduit donc à prouver que

$$\left[\frac{L}{-q}\right] = \left[\frac{-q}{L}\right] \quad \text{et} \quad \left[\frac{L}{p}\right] = \left[\frac{p}{L}\right].$$

En se servant toujours de la seconde et de la troisième formule de décomposition (24.), la première proposition résulte immédiatement du Théorème IV. et du Lemme II. Quant à la seconde, elle se déduit de l'équation (18.), c'est a dire de l'équation $\left[\frac{h_1^2 h_2}{p_1}\right] = \left[\frac{p^2}{h_1}\right]$, où p, h sont des nombres prémiers réels $4n+1$, et où $p = p_1 p_2$, $h = h_1 h_2$; p_1, p_2, h_1, h_2 étant des nombres premiers complexes de seconde espèce ayant resp. p, h pour normes communes. En effet h_1, h_2 étant conjugués et p étant réel, le Lemme I. donne

$$\left[\frac{h_1^2}{p_1}\right] = \left[\frac{h_2}{p_2}\right], \quad \left[\frac{p^2}{h_1}\right] = \left[\frac{p}{h_2}\right];$$

donc il vient

$$\left[\frac{h_2}{p_2}\right]\left[\frac{h_2}{p_1}\right] = \left[\frac{h_2}{p}\right] = \left[\frac{p}{h_2}\right].$$

Or désignant par B le plus grand entier réel qui divise L, et par h_2, h_2', h_2'' etc. les autres facteurs simples de seconde espèce de L, on aura

$$L = B h_2 h_2' h_2'' \ldots,$$

$$\left[\frac{L}{p}\right] = \left[\frac{B}{p}\right]\left[\frac{h_2}{p}\right]\left[\frac{h_2'}{p}\right]\left[\frac{h_2''}{p}\right] \ldots$$

$$\left[\frac{p}{L}\right] = \left[\frac{p}{B}\right]\left[\frac{p}{h_2}\right]\left[\frac{p}{h_2'}\right]\left[\frac{p}{h_2''}\right] \ldots;$$

mais $\left[\frac{B}{p}\right] = \left[\frac{p}{B}\right] = 1$ (Lem. II.), et de plus $\left[\frac{h_2}{p}\right] = \left[\frac{p}{h_2}\right]$, $\left[\frac{h_2'}{p}\right] = \left[\frac{p}{h_2'}\right]$, $\left[\frac{h_2''}{p}\right] = \left[\frac{p}{h_2''}\right]$ etc. en vertu de ce que nous venons de trouver: donc aussi

$$\left[\frac{L}{p}\right] = \left[\frac{p}{L}\right].$$

Lemme IV. „Désignant par m un entier réel impair positif ou négatif, on a $\left[\frac{i}{m}\right] = 1$ pour $m \equiv 1, 7 \pmod{8}$ et $\left[\frac{i}{m}\right] = -1$ pour $m \equiv 3, 5 \pmod{8}$, ou, ce qui revient au même, on a toujours $\left[\frac{i}{m}\right] = \left(\frac{2}{m}\right)$. De là comme corollaire il suit que

$$\left[\frac{i}{m}\right]\left[\frac{i}{m'}\right] = 1, \text{ lorsque } m \equiv m' \pmod{8}, \text{ et}$$

$$\left[\frac{i}{m}\right]\left[\frac{i'}{m'}\right] = -1, \text{ lorsque } m \equiv m'+4 \pmod{8}."$$

Soit $p = p_1 p_2$ un nombre premier positif $4n+1$, on aura (Lemme I.) $\left[\frac{i}{p_2}\right] = \left[\frac{-i}{p_1}\right]^3$; multipliant par $\left[\frac{i}{p_1}\right]$ il vient

$$\left[\frac{i}{p}\right] = \left[\frac{-i}{p_1}\right]^3\left[\frac{i}{p_1}\right] = \left[\frac{-1}{p_1}\right] = (-1)^{\frac{1}{4}(p-1)};$$

donc $\left[\frac{i}{p}\right] = +1$ ou $= -1$, selon que $p \equiv 1$ ou $\equiv 5 \pmod{8}$, et par conséquent $\left[\frac{i}{\pm p}\right] = +1$ ou $= -1$, selon que $p \equiv \pm 1$ ou $p \equiv \pm 5 \pmod{8}$, c'est à dire selon que $\pm p \equiv 1, 7$ ou $\pm p \equiv 3, 5 \pmod{8}$. Soit en second lieu q un nombre premier positif $4n+3$, on aura

$$\left[\frac{i}{\pm q}\right] = i^{\frac{1}{4}(q^2-1)} = (-1)^{\frac{1}{8}(q^2-1)}, \text{ donc } \left[\frac{i}{\pm q}\right] = \left(\frac{2}{\pm q}\right).$$

Quel que soit donc le nombre premier réel (a) on aura toujours $\left[\frac{i}{\pm \mathrm{a}}\right] = \left(\frac{2}{\pm \mathrm{a}}\right)$. Celà étant, on peut toujours supposer

$$m = \pm \mathrm{a}\,\mathrm{a}'\,\mathrm{a}'' \ldots.$$

où a, a, a″, ... sont les facteurs simples réels de m; il suit donc que

$$\left[\frac{i}{m}\right] = \left[\frac{i}{\mathrm{a}}\right]\left[\frac{i}{\mathrm{a}'}\right]\left[\frac{i}{\mathrm{a}''}\right] \ldots = \left(\frac{2}{\mathrm{a}}\right)\left(\frac{2}{\mathrm{a}'}\right)\left(\frac{2}{\mathrm{a}''}\right) \ldots = \left(\frac{2}{m}\right).$$

ce qu'il s'agissoit de prouver.

Nous considérerons dorénavant avec Mr. *Gauss* comme nombre *primaire* parmi quatre entiers complexes impairs *associés* qui forment un même groupe, celui $a+bi$, évidemment unique, pour lequel on a

ou $a \equiv 1 \pmod{4}$, et en même temps $b \equiv 0 \pmod{4}$,
ou $a \equiv 3 \pmod{4}$, et en même temps $b \equiv 2 \pmod{4}$.

Mais cette expression ne doit pas être confondue avec ce que Mr. *Dirichlet* appelle nombre primaire. On conclura aisément de la convention que nous venons de poser, que le produit de deux, et par conséquent d'un nombre quelconque d'entiers primaires est lui même un entier primaire. Tous les entiers primaires peuvent être distribués en deux classes distinctes, en comprenant dans la *première classe* tous ceux qui sont $\equiv 1 \pmod{4}$ et dans la

seconde tous ceux qui sont $\equiv 3+2i$ (mod. 4). Cette distinction est d'une grande utilité dans la théorie des résidus biquadratiques, et il sera bon de l'appliquer à des exemples.

Les entiers ***réels*** impairs, pour être ***primaires,*** doivent être pris avec le signe ***plus,*** ou avec le signe ***moins,*** selon qu'ils sont, abstraction faite du signe, $\equiv 1$ (mod. 4) ou $\equiv 3$ (mod. 4). Les entiers réels et primaires appartiennent donc toujours à la première classe, puisque leur partie imaginaire est zéro, et partant $\equiv 0$ (mod. 4).

Ces préliminaires posés, soient $a+bi$ et $c+di$ deux entiers complexes primaires premiers entre eux dont les éléments a et b, c et d ***n'ont pas de diviseur commun.*** Cela étant, on aura évidemment la congruence

$$(A.)\quad c^4(a+bi) \equiv c^3(ac+bd) \pmod{c+di}.$$

En effet, la différence des deux membres est $= ac^4+bc^4i-ac^4-bc^3d = bc^4i-bc^3d = bc^3i(c+di)$ et parsuite divisible par le module $c+di$. Suivant l'hypothèse admise sur les entiers c et d, c n'aura pas de diviseur commun avec le module; mais $a+bi$ étant également premier à $c+di$, le premier membre de la congruence $(A.)$, et par suite aussi le second, n'auront pas de diviseur commun avec le module. On tirera donc de là l'équation

$$(B.)\quad \left[\frac{a+bi}{c+di}\right] = \left[\frac{c}{c+di}\right]^3 \left[\frac{ac+bd}{c+di}\right].$$

Les entiers a et b n'ayant pas également de diviseur commun, on aura de même

$$(C.)\quad \left[\frac{c+di}{a+bi}\right] = \left[\frac{a}{a+bi}\right]^3 \left[\frac{ac+bd}{a+bi}\right]$$

et partant (Lemme I.)

$$(D.)\quad \left[\frac{c+di}{a+bi}\right]^3 = \left[\frac{a}{a+bi}\right] \left[\frac{ac+bd}{a-bi}\right].$$

Multipliant entre elles les équations $(B.)$ et $(D.)$, il vient

$$(E.)\quad \left[\frac{a+bi}{c+di}\right]\left[\frac{c+di}{a+bi}\right]^3 = \left[\frac{c}{c+di}\right]^3 \left[\frac{a}{a+bi}\right]\left[\frac{ac+bd}{(c+di)(a-bi)}\right].$$

Pour pouvoir appliquer *le troisième Lemme* au second membre de cette équation, il faut que les numérateurs des symboles qui y entrent soient $\equiv 1$ (mod. 4). Soit donc pour abréger $\delta = \pm 1$, $\varepsilon = \pm 1$, où les signes sont pris tels, qu'on ait

$$a \equiv \delta \pmod{4}, \qquad c \equiv \varepsilon \pmod{4}.$$

Cela posé, on aura $\varepsilon c \equiv 1$ (mod. 4), $\delta a \equiv 1$ (mod. 4), $\delta\varepsilon(ac+bd) \equiv \delta\varepsilon ac \equiv 1$ (mod. 4). Donnons donc au second membre de l'équation $(E.)$ la forme

$$(F.)\quad \left[\frac{\varepsilon c}{c+di}\right]^2\left[\frac{\delta a}{a+bi}\right]\left[\frac{\delta\varepsilon(ac+bd)}{ac+bd+i(ad-bc)}\right]\left[\frac{\varepsilon}{a+bi}\right]\left[\frac{\delta}{c+di}\right]:$$

forme dont la legitimité résulte de ce que $\delta^2=\varepsilon^2=1$. Comme les numérateurs des trois premiers symboles sont ici des entiers réels et $\equiv 1 \pmod 4$, on pourra (Lemme III.) remplacer ces trois symboles respectivement par les symboles inverses

$$(G.)\quad \left[\frac{c+di}{c}\right]^2,\quad \left[\frac{a+bi}{a}\right],\quad \left[\frac{ac+bd+i(ad-bc)}{ac+bd}\right],$$

respectivement équivalents aux suivants:

$$\left[\frac{di}{c}\right]^2=\left[\frac{i}{c}\right]^2=\left[\frac{i}{c}\right],\quad \left[\frac{bi}{a}\right]=\left[\frac{i}{a}\right],\quad \left[\frac{i(ad-bc)}{ac+bd}\right]=\left[\frac{i}{ac+bd}\right],$$

de sorte que la valeur du produit des trois premiers termes qui entrent dans l'expression $(F.)$ se réduit à

$$(H.)\quad \left[\frac{i}{ac}\right]\left[\frac{i}{ac+bd}\right].$$

Il reste encore les deux derniers facteurs du produit $(F.)$. Je dis que le produit de ces deux facteurs se réduit toujours à l'unité prise positivement. En effet, comme l'on a $\varepsilon=(-1)^{\frac12(c-1)}$, $\delta=(-1)^{\frac12(a-1)}$, le produit dont il s'agit peut s'écrire ainsi:

$$\left[\frac{-1}{a+bi}\right]^{\frac12(c-1)}\left[\frac{-1}{c+di}\right]^{\frac12(a-1)}.$$

Or

$$\left[\frac{-1}{a+bi}\right]=(-1)^{\frac12(a-1)},\quad \left[\frac{-1}{c+di}\right]=(-1)^{\frac12(c-1)},$$

donc

$$(-1)^{\frac12(a-1)\frac12(c-1)}\cdot(-1)^{\frac12(c-1)\frac12(a-1)}=+1.$$

Toute la valeur du second membre de l'équation $(E.)$ se réduit donc à l'expression $(H.)$. Cherchons la valeur de cette expression. Lorsque les entiers complexes primaires $a+bi$ et $c+di$ n'appartiennent pas tous deux à la seconde classe, le produit bd sera nécessairement divisible par 8, d'où l'on tire $ac\equiv ac+bd \pmod 8$, et l'expression $(H.)$ aura la valeur $+1$. Mais si les nombres $a+bi$ et $c+di$ appartiennent tous les deux à la seconde classe, b et d seront de la forme $4n+2$ et par conséquent bd sera de la forme $8n+4$, et parsuite $ac\equiv ac+bd+4 \pmod 8$, et l'expression $(H.)$ se réduira à -1 (Lemme IV.).

Or multipliant l'équation $(E.)$ de part et d'autre par $\left[\frac{c+di}{c+di}\right]$ et ob-

servant que $\left[\frac{c+di}{a+bi}\right]^4 = 1$, on voit que les deux expressions

$$(I.)\quad \left[\frac{a+bi}{c+di}\right] \text{ et } \left[\frac{c+di}{a+bi}\right]$$

sont ou égales ou opposées, selon que les deux entiers primaires qui y entrent n'appartiennent pas ou appartiennent tous les deux à la seconde classe.

Pour généraliser encore le résultat que nous venons de trouver, soient

$$A+Bi = \mu(a+bi),\quad C+Di = \nu(c+di)$$

deux entiers complexes quelconques primaires premiers entre eux, μ et ν étant deux entiers réels que nous supposons tous les deux $\equiv 1$ (mod. 4), et $a+bi$, $c+di$ ayant la même signification que dans ce qui précède; il n'existe pas de nombre primaire, qui ne soit pas représenté sous cette forme. Cela posé, les équations (24.) donnent

$$\left[\frac{A+Bi}{C+Di}\right] = \left[\frac{\mu}{\nu}\right]\left[\frac{\mu}{c+di}\right]\left[\frac{a+bi}{\nu}\right]\left[\frac{a+bi}{c+di}\right],$$

$$\left[\frac{C+Di}{A+Bi}\right] = \left[\frac{\nu}{\mu}\right]\left[\frac{c+di}{\mu}\right]\left[\frac{\nu}{a+bi}\right]\left[\frac{c+di}{a+bi}\right].$$

Or $\left[\frac{\mu}{\nu}\right] = \left[\frac{\nu}{\mu}\right]$ (Lemme II.), $\left[\frac{\mu}{c+di}\right] = \left[\frac{c+di}{\mu}\right]$, $\left[\frac{\nu}{a+bi}\right] = \left[\frac{a+bi}{\nu}\right]$ (Lemme III.), et enfin d'après ce que nous venons de trouver,

$$\left[\frac{a+bi}{c+di}\right] = -\left[\frac{c+di}{a+bi}\right] \quad \text{ou} \quad = +\left[\frac{c+di}{a+bi}\right],$$

selon que $a+bi$ et $c+di$ appartiennent ou n'appartiennent pas tous les deux à la seconde classe, ou ce qui revient au même, μ et ν étant $\equiv 1$ (mod. 4), selon que $A+Bi$ et $C+Di$ appartiennent ou n'appartiennent pas tous les deux à la seconde classe. Il vient donc selon ces deux cas

$$\left[\frac{A+Bi}{C+Di}\right] = \mp\left[\frac{C+Di}{A+Bi}\right],$$

c'est à dire

$$\left[\frac{A+Bi}{C+Di}\right] = (-1)^{\frac{1}{4}(A-1)\cdot\frac{1}{4}(C-1)}\cdot\left[\frac{C+Di}{A+Bi}\right].$$

Théorème fondamental.* „*Désignant par $A+Bi$ et $C+Di$ deux „entiers complexes primaires sans diviseur commun, c'est à dire tels que „l'on ait, ou simultanément $A\equiv 1$, $B\equiv 0$ (mod. 4), ou simultanément „$A\equiv 3$, $B\equiv 2$ (mod. 4), ou, ce qui revient au même, tels que l'on ait „$A+Bi\equiv C+Di\equiv 1$ (mod. $2+2i$), le caractère biquadratique du premier

„par rapport au second est égal au caractère biquadratique du second „par rapport au premier, lorsque ou l'un et l'autre ou du moins l'un „des deux est $\equiv 1$ (mod. 4); *mais ces caractères biquadratiques diffèrent „de deux unités, lorsque* $A+Bi$ *et* $C+Di$ *sont tous les deux* $\equiv 3+2i$ „(mod. 4)."

On voit que ce théorème comprend comme cas particulier le théorème célèbre de Mr. *Gauss*, que ce profond analyste a énoncé dans le §. 67. de ses recherches sur les résidus biquadratiques. Voici donc la démonstration rigoureuse et générale de ce théorème celèbre, laquelle l'illustre auteur que nous venons de citer juge sujette à de si grandes difficultés, qu'il la renvoie aux plus profonds mystères de l'arithmétique transcendante *). Néanmoins il y a d'autant plus lieu de s'étonner que personne n'a songé d'en exposer une démonstration, puisque toute la théorie des nombres complexes paraît être inventée, pour ainsi dire, en faveur de ce théorème.

La démonstration que nous venons de présenter est très simple, et quoique elle paraît être un peu longue, on remarquera que nous n'avons presque rien supposé connu, excepté quelques formules fort simples que nous avons prouvées dans un autre lieu déjà cité, et dont la démonstration repose sur ce seul principe qu'un système de résidus, multiplié par un entier premier au module, reproduit un système de résidus. Au reste je suis parvenu encore à une autre démonstration de ce théorème excellent, que j'exposerai plus tard.

Parmi les conséquences nombreuses du théorème que nous venons d'énoncer, nous ne citerons qu'une seule qui est surtout remarquable et dont la démonstration se présente facilement.

„Désignant par L un entier complexe impair donné, par z un entier complexe variable: tous lès facteurs complexes simples premier à L qui divisent la forme $z^4 - L$ sont contenus dans un nombre déterminé de formules linéaires telles que $4Ly + b$, où y est un entier complexe variable et b un entier complexe déterminé.

Remarque. Dans les recherches qui précèdent nous avons souvent employé la conclusion suivante:

---

*) Voici ses propres mots: „At non obstante summa hujus theorematis simplicitate, ipsius demonstratio inter mysteria arithmeticae sublimioris maxime recondita referenda est, ita ut, saltem ut nunc res est, subtilissimas tantummodo investigationes enodari possit, quae limites praesentis commentationis longe transgrederentur." La troisième partie de ces recherches, à laquelle l'illustre auteur renvoie sa démonstration, n'a pas encore paru.

„Le produit d'un entier complexe α et d'une fonction entière de r à coëfficients entiers complexes étant égal à un autre entier complexe β, et cette égalité subsistant quelle que soit la racine r de l'équation $\frac{x^p-1}{x-1}=0$, il suit de là que β est nécessairement divisibe par α."

La légitimité de cette conclusion peut être démontrée aisément comme suit. Chaque fonction entière de r, telle que nous venons de définir, peut prendre la forme

$$A+Br+Cr^2+\ldots+Kr^{p-1},$$

$A, B, C, \ldots K$ étant des entiers complexes; on a donc suivant l'hypothese

$$\alpha(A+Br+Cr^2+\ldots+Kr^{p-1}) = \beta,$$
$$\alpha(A+Br^2+Cr^4+\ldots+Kr^{2(p-1)}) = \beta,$$
$$\cdots\cdots\cdots\cdots$$
$$\alpha(A+Br^{p-1}+Cr^{2(p-1)}+\ldots+Kr^{(p-1)^2}) = \beta.$$

En multipliant ces équations resp. par $r, r^2, \ldots r^{p-1}$, et les ajoutant, il vient

$$\alpha(-A-B-C-\ldots+(p-1)K) = -\beta,$$

donc β est divisible par α, ce qu'il s'agissait de prouver.

Berlin, Juin 1844.

10.

Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln.

(Von Herrn Dr. *Otto Hesse*, Privatdocenten an der Universität zu Königsberg.)

---

1) Wenn man aus zwei gegebenen vollständigen Gleichungen mit einer Variable vom $m$ten und $n$ten Grade diese Variable auf irgend eine Weise eliminirt, so erhält man eine Gleichung zwischen den Coëfficienten der gegebenen Gleichungen, welche erfüllt wird, sobald ein Werth der Variable den beiden gegebenen Gleichungen zugleich genügt. Wenn umgekehrt diese Gleichung zwischen den Coëfficienten erfüllt wird, so braucht nicht immer ein Werth der Variable zu existiren, der den beiden gegebenen Gleichungen zugleich genügt. Durch eine geschickt angestellte Elimination der Variable kann man aber eine Bedingungsgleichung zwischen den Coëfficienten der gegebenen Gleichungen finden, unter welcher jedesmal ein Werth der Variable existirt, welcher den gegebenen Gleichungen zugleich genügt, und die erfüllt wird, wenn ein Werth der Variable die beiden gegebenen Gleichungen zugleich erfüllt. Diese Gleichung, die in allen durch Elimination der Variable entstandenen Gleichungen als Factor enthalten ist, führt den Namen der Endgleichung, während die andern Factoren mit dem Namen der überflüssigen Factoren bezeichnet werden. Durch *Euler* (Mem. d. Berl Akad. an. 1748 und 1760) ist bekannt, dafs die Endgleichung homogen ist und in Rücksicht auf die Coëfficienten der Gleichung vom $m$ten Grade bis auf den $n$ten, in Rücksicht auf die Coëfficienten der Gleichung vom $n$ten Grade bis auf den $m$ten, endlich in Rücksicht auf alle Coëfficienten der gegebenen Gleichungen bis auf den $(m+n)$ten Grad steigt. Unter den bekannten Verfahrungsweisen, die Endgleichung zu bilden, verdient die Zurückführung der Aufgabe auf die Elimination der Unbekannten aus linearen Gleichungen, welche der Herr Professor *Richelot* als einer Entdeckung des Herrn *Sylvester* in dem 21ten Bande dieses Journals erwähnt, und welche ich ohne sie zu kennen im 27ten Bande wieder aufgenommen habe, unstreitig den Vorzug.

Für drei Gleichungen mit zwei Variabeln ist, soviel ich weiß, Ähnliches noch nicht geleistet worden. Ich werde daher im Folgenden die *Euler*sche Methode zu verallgemeinern suchen.

2) Es seien:

$$1.\quad f(x,y) = 0,\qquad 2.\quad \varphi(x,y) = 0,\qquad 3.\quad \psi(x,y) = 0$$

drei vollständige Gleichungen zwischen den beiden Variabeln x und y, vom $m$ten, $n$ten und $p$ten Grade. Diesen Gleichungen wird man im Allgemeinen nicht durch *ein* Wurzelpaar x und y genügen können, wenn nicht eine bestimmte Relation zwischen den Coëfficienten der gegebenen Gleichungen stattfindet, und wenn diese Relation stattfindet, wird man immer *ein* Wurzelpaar finden, welches den gegebenen Gleichungen zu gleicher Zeit genügt. Um diese Relation zu finden, welche im Folgenden den Namen der Endgleichung führen wird, suche man die Bedingung zwischen den Coëfficienten der 3ten Gleichung, unter welcher ein Wurzelpaar der beiden ersten Gleichungen der dritten Gleichung genügt.

Unter der Voraussetzung, daß $m.n$ die Anzahl der Wurzelpaare der beiden ersten Gleichungen ist, was *Euler* an dem genannten Orte bewiesen hat, ist die gesuchte Bedingung:

$$4.\quad \Psi = \psi(x_1, y_1).\psi(x_2, y_2)\ \ldots\ldots\ \psi(x_{m.n}, y_{m.n}) = 0,$$

wenn man durch x_1, y_1; x_2, y_2; .... $x_{m.n}, y_{m.n}$ die Wurzelpaare der ersten und zweiten Gleichung bezeichnet. Denn wenn ein Wurzelpaar der beiden ersten Gleichungen zugleich der dritten genügt, so wird auch die Gleichung (4.) erfüllt; und umgekehrt, wenn die Gleichung (4.) erfüllt wird, so giebt es immer ein Wurzelpaar der beiden ersten Gleichungen, welches der dritten Gleichung genügt. Entwickelt man den linken Theil der Gleichung (4.) nach Potenzen und Producten der Coëfficienten der dritten Gleichung, welche Entwicklung mit Ψ bezeichnet werden mag, so wird die Gleichung $\Psi = 0$ in Rücksicht auf die Coëfficienten der dritten Gleichung homogen und vom Grade $m.n$ und die Coëfficienten dieser Potenzen und Producte werden bestimmte Functionen der Wurzeln der beiden ersten Gleichungen sein. Es bleibt also noch übrig, diese Functionen in der Entwicklung Ψ durch die Coëfficienten der beiden ersten Gleichungen auszudrücken, um die gesuchte, von jedem überflüssigen Factor freie Endgleichung zu erhalten.

3) Wenn man auf irgend eine Weise aus den drei gegeben Gleichungen die Variabeln eliminirt, so erhält man eine Gleichung

$$5.\quad P = 0,$$

welche immer erfüllt wird, sobald ein Wurzelpaar den drei gegebenen Glei-

chungen zugleich genügt Den drei gegebenen Gleichungen wird aber durch ein Wurzelnpaar genügt, wenn die Gleichung (4.) erfüllt wird. Daraus folgt, dafs die Gleichung (5.) erfüllt wird, wenn die Gleichung (4.) erfüllt wird. Angenommen, dafs man die Gleichung (5.) gefunden habe, und dafs sie in Rücksicht auf die Coëfficienten der dritten Gleichung homogen und vom Grade $m.n$ sei. Da dieselbe für alle Werthe der Coëfficienten der dritten Gleichung erfüllt wird, welche der Gleichung (4.) nugthun, so folgt hieraus, dafs die Ausdrücke P und Ψ nur durch einen von den Coëfficienten der dritten Gleichung unabhängigen Factor von einander verschieden sein können. Bezeichnet man daher das in der Function ψ von den Variabeln x, y freie Glied mit c und den Coëfficienten $c^{m.n}$ in der Entwicklung der Function P mit γ, so wird man

$$6. \quad \frac{P}{\gamma} = \Psi$$

haben, woraus sich durch Gleichsetzung der Coëfficienten gleicher Potenzen und Producte der Coëfficienten der dritten Gleichung auf beiden Seiten der angeführten Gleichung die gesuchten Functionen der Wurzeln, ausgedrückt durch die Coëfficienten der beiden ersten Gleichungen, ergeben. Es kommt also darauf an, aus den drei gegebenen Gleichungen durch eine geschickt angestellte Elimination der Variabeln eine homogene Gleichung $P=0$ vom mnten Grade in Rücksicht auf die Coëfficienten der dritten Gleichung abzuleiten. Man wird sogleich sehen, wie dies auszuführen sei, wenn die 3te Gleichung vom ersten Grade ist.

4) Es sei die gegebene dritte Gleichung

$$7. \quad \psi_\lambda(x, y) = a_\lambda x + b_\lambda y + c_\lambda = 0$$

lineär. Alsdann geht die Gleichung (4.) in

$$8. \quad \Psi_\lambda = (a_\lambda x_1 + b_\lambda y_1 + c_\lambda)(a_\lambda x_2 + b_\lambda y_2 + c_\lambda) \ldots . (a_\lambda x_{m.n} + b_\lambda y_{m.n} + c_\lambda) = 0$$

über. Man eliminirt aber die Variable y aus den gegebenen drei Gleichungen, indem man aus der letzten den Werth

$$y = -\frac{a_\lambda x + c_\lambda}{b_\lambda}$$

in die beiden ersten setzt, wodurch man, wenn man mit b^m und b^n multiplicirt, folgende in Rücksicht auf a_λ, b_λ, c_λ homogene Gleichungen

$$9. \quad b_\lambda^m f\left(x_\lambda, -\frac{a_\lambda x + c_\lambda}{b_\lambda}\right) = 0, \qquad b_\lambda^n \varphi\left(x_\lambda, -\frac{a_\lambda x + c_\lambda}{b_\lambda}\right) = 0$$

erhält. Diese Gleichungen sind in Rücksicht auf a_λ, b_λ, c_λ respective vom $m$ten und vom $n$ten Grade, so wie auch in Rücksicht auf die Variable x.

Eliminirt man daher die noch übrig bleibende Variable x nach der bekannten Methode, so wird man eine Gleichung

$$10.\quad P_\lambda = 0$$

erhalten, welche in Rücksicht auf die Coëfficienten in f, φ, ψ_λ respective vom $n$ten, $m$ten und $m.n$ten, in Rücksicht auf die Coëfficienten in f und φ vom $m+n$ten und in Rücksicht auf alle Coëfficienten homogen und vom Grade $m+n+m.n$ ist. Bezeichnet man daher durch g den Coëfficienten von $c_\lambda^{m.n}$ in der Entwicklung des nach Potenzen und Producten der Gröſsen a_λ, b_λ, c_λ geordneten Ausdrucks P_λ, der in Rücksicht auf die Coëfficienten in f und φ vom $n$ten und vom $m$ten und in Rücksicht auf beiderlei Coëfficienten vom Grade $m+n$ ist, so erhält man:

$$11.\quad \frac{P_\lambda}{g} = \Psi_\lambda.$$

Entwickelt man beide Seiten der Gleichung nach Potenzen und Producten der Gröſsen a_λ, b_λ, c_λ und setzt die Coëfficienten gleicher Potenzen und Producte auf beiden Seiten der Gleichung einander gleich, so erhält man Functionen der Wurzeln der beiden ersten Gleichungen, welche sich in der Entwicklung Ψ der Gleichung (4.) wiederfinden, ausgedrückt durch die Coëfficienten jener beiden Gleichungen. Auf diese Weise kann man aber nur gewisse Functionen der Wurzeln, welche in der Entwicklung Ψ enthalten sind, durch die Coëfficienten der beiden ersten Gleichungen ausdrücken. Um alle jene Functionen der Wurzeln auszudrücken, nehme man statt der linearen Gleichung (7.) nach einander die linearen Gleichungen

$$\psi_1(x,y) = 0,\quad \psi_2(x,y) = 0,\quad \ldots\ldots\ \psi_p(x,y) = 0,$$

welche aus jener entstehen, indem man für den Index λ nach einander die Indices 1, 2, ... p setzt, und bilde die ihnen entsprechenden Gleichungen (8. bis 11.), welche durch die entsprechenden Indices bezeichnet werden sollen. Endlich nehme man an, daſs die gegebene dritte Gleichung in die linearen Factoren $\psi_1(x,y)$, $\psi_2(x,y)$, ... $\psi_p(x,y)$ zerfällbar sei.

5) Wenn die gegebene dritte Gleichung

$$12.\quad \psi_1(x,y)\,.\,\psi_2(x,y)\ldots\,.\,\psi_p(x,y) = 0$$

ist, so geht die Gleichung (4.) in

$$13.\quad \Psi_1\Psi_2\ldots\Psi_p = 0$$

über, und wenn ein Wurzelpaar den Gleichungen (1.), (2.), (12.) zugleich genügt, so hat man

$$14.\quad P_1P_2\ldots P_p = 0.$$

Dennoch wird die Gleichung (14.) erfüllt für alle Werthe von a_1, b_1, c_1, a_2, b_2, ..., welche der Gleichung (13.) genügen. Es können daher die linken Theile derselben, welche in Rücksicht auf die genannten Gröfsen homogen und von demselben Grade sind, nur durch einen von a_1, b_1, ... unabhängigen Factor sich von einander unterscheiden. Bezeichnet man also durch Ψ_0 und P_0 die linken Theile jener Gleichungen, so hat man

$$15. \quad \frac{P_0}{g^p} = \Psi_0.$$

Entwickelt man beide Theile dieser Gleichung nach Potenzen und Producten der Gröfsen a_1, b_1, c_1, a_2, b_2, ... und setzt die Coëfficienten gleicher Potenzen und Producte auf beiden Seiten der Gleichung einander gleich, so erhält man gerade die gesuchten Functionen der Wurzeln der beiden ersten Gleichungen, welche in der Entwicklung des linken Theils der Gleichung (4.) vorkommen, ausgedrückt durch die Coëfficienten der Gleichungen (1.) und (2.). Alle diese Ausdrücke haben den gemeinschaftlichen Nenner g^p, welcher in Rücksicht auf die Coëfficienten der ersten und zweiten Gleichung homogen und respective vom np und mpten, und überhaupt vom $(m+n)p$ten Grade ist. Da nun, wie man gesehen hat, die Coëfficienten der Entwicklung von P_λ nach Potenzen und Producten von a_λ, b_λ, c_λ in Rücksicht auf die Coëfficienten der ersten und zweiten Gleichung vom $n$ten und $m$ten Grade sind, so wird P_0 respective vom np und mpten und in Rücksicht auf alle Coëfficienten der ersten und zweiten Gleichung vom Grade $(m+n)p$ sein. Dasselbe gilt von den Zählern der Ausdrücke für die genannten Functionen der Wurzeln der ersten und zweiten Gleichung.

6) Die aus den gegebenen Gleichungen (1.), (2.), (3.) hervorgehende Endgleichung erhält man nun aus der entwickelten Gleichung (4.), wenn man darin die Ausdrücke der Functionen der Wurzeln der beiden ersten Gleichungen substituirt und mit dem gemeinsamen Nenner g^p derselben multiplicirt. Aus dieser Bildungsweise der Endgleichung ergiebt sich aber folgender

Lehrsatz 1.

Die durch Elimination zweier Variabeln aus drei algebraischen Gleichungen vom $m$ten, $n$ten und $p$ten Grade hervorgehende Endgleichung ist in Rücksicht auf alle Coëfficienten dieser Gleichungen homogen und vom Grade $mn+np+pm$, und in Rücksicht auf die Coëfficienten der einzelnen Gleichungen ebenfalls homogen und von den Graden mn, np, pm.

7) Obwohl die auseinandergesetzte Eliminationsmethode immer zum Ziele führt, so lassen sich die angewendeten Operationen wegen ihrer Unsymmetrie doch zu wenig verfolgen, als dafs man daraus die wahre Natur der Endgleichung mit Leichtigkeit erforschen könnte. Da die Endgleichung, selbst in dem Falle wo die gegebenen Gleichungen sämmtlich nur vom zweiten Grade sind, aus einer nicht übersehbaren Menge von Termen besteht, welche *Bézout* in seiner Theorie der algebraischen Gleichungen nicht ohne Mühe berechnet hat, so wird man es nicht versuchen, aus der Endgleichung selbst Nutzen zu ziehen, vielmehr symmetrische und leicht zu verfolgende Eliminationsmethoden sich schaffen müssen, die eine Einsicht in die Natur der Endgleichung gestatten. Für den Fall dreier Gleichungen vom zweiten Grade mit zwei Variabeln werde ich eine solche Methode entwickeln, und zugleich Folgerungen ziehen, die für die Theorie der Wendepuncte der Curven dritter Ordnung wichtig sind. Denn während die Bestimmung der Wendepuncte der Curven dritter Ordnung auf eine Gleichung vom 9ten Grade führt, bietet die genannte Eliminations-Methode die Mittel, diese Gleichung vom 9ten Grade durch eine vom 4ten und eine Gleichung vom 3ten Grade zu ersetzen. Von den geometrischen Eigenschaften der Curven dritter Ordnung, welche sich aus dieser Eliminations-Methode ergeben, führe ich vorläufig nur diese an: „Dafs die *Wendepuncte* aller Curven dritter Ordnung, von denen jede durch sämmtliche Wendepuncte einer und derselben Curve derselben Ordnung hindurchgeht, mit den *Schnittpuncten* zusammenfallen."

8) Wenn man durch f_1, f_2, f_3 drei gegebene homogene Functionen vom zweiten und durch φ und ψ zwei gegebene homogene Functionen vom dritten Grade der drei Variabeln x_1, x_2, x_3 bezeichnet, so kann man immer drei lineäre homogene Multiplicatoren $A^{(1)}$, $A^{(2)}$, $A^{(3)}$ und einen constanten Multiplicator p so bestimmen, dafs

$$p\varphi+A^{(1)}f_1+A^{(2)}f_2+A^{(3)}f_3 = \psi$$

ist. Denn wenn man die Coëfficienten gleicher Potenzen und Producte der Variabeln auf beiden Seiten der entwickelten Gleichung einander gleich setzt, so erhält man 10 lineäre Gleichungen zwischen den 9 in $A^{(1)}$, $A^{(2)}$, $A^{(3)}$ enthaltenen Constanten und der 10ten p. Bestimmt man daraus die unbekannten 10 Constanten, so stellen sich die Werthe derselben als Brüche dar, mit demselben Nenner R. Dieser Nenner ist unabhängig von den Coëfficienten der Variabeln in der Function ψ; er ist homogen und lineär in Rücksicht auf die Coëfficienten in φ; ferner ist er homogen und vom 3ten Grade, sowohl in Rücksicht auf die Coëfficienten

in f_1, als in Rücksicht auf die Coëfficienten in f_2 und f_3; endlich ist er homogen und vom 10ten Grade in Rücksicht auf alle in f_1, f_2, f_3 und φ enthaltenen Coëfficienten. Was den Zähler des Werthes der Unbekannten p betrifft, so kann man die Bemerkung machen, dafs er unabhängig von den Coëfficienten in φ ist, homogen aber und vom ersten Grade in Rücksicht auf die Coëfficienten in ψ, homogen und vom dritten Grade sowohl in Rücksicht auf die Coëfficienten in f_1 als in f_2 und f_3; endlich homogen und vom 10ten Grade in Rücksicht auf alle in f_1, f_2, f_3, ψ enthaltenen Coëfficienten.

Die Nenner der unbekannten Coëfficienten lassen sich vermeiden, wenn man $R.\psi$ statt ψ setzt, wodurch die in Rede stehende Gleichung in

$$16. \quad p\varphi + A^{(1)}f_1 + A^{(2)}f_2 + A^{(3)}f_3 = R.\psi$$

übergeht. Denn bestimmt man in der angegebenen Weise die unbekannten Coëfficienten in dieser Gleichung, so werden dieselben gleich den Zählern der unbekannten Coëfficienten in der vorhergehenden Gleichung, und folglich zu ganzen Functionen der in f_1, f_2, f_3, φ und ψ enthaltenen Coëfficienten.

Da die Gröfse R unabhängig von den Coëfficienten in ψ ist, so wird sich dieselbe auch nicht ändern, wenn man für ψ das Product $x_\varkappa . x_\lambda . x_\mu$ setzt, wo $\varkappa$, λ, μ irgend welche gleiche oder ungleiche unter den Zahlen 1, 2, 3 bedeuten. Die andern Multiplicatoren werden sich aber ändern und mögen durch $p_{\varkappa,\lambda,\mu}$, $A^{(1)}_{\varkappa,\lambda,\mu}$, $A^{(2)}_{\varkappa,\lambda,\mu}$, $A^{(3)}_{\varkappa,\lambda,\mu}$ bezeichnet werden, wobei angenommen werden soll, dafs die verschiedenen Zeichen, welche aus den angegebenen durch Permutation der unteren Indices unter einander entstehen, immer für dieselbe Gröfse gelten, so dafs z. B.

$$p_{\varkappa,\lambda,\mu} = p_{\varkappa,\mu,\lambda} = p_{\lambda,\varkappa,\mu} = \dots\dots$$

ist. Dasselbe soll auch künftig für alle ähnlichen Bezeichnungen gelten.

Demnach hat man

$$17. \quad p_{\varkappa,\lambda,\mu}\varphi + A^{(1)}_{\varkappa,\lambda,\mu}f_1 + A^{(2)}_{\varkappa,\lambda,\mu}f_2 + A^{(3)}_{\varkappa,\lambda,\mu}f_3 = R x_\varkappa x_\lambda x_\mu,$$

woraus sich, wenn man für $\varkappa$, λ, μ alle Combinationen der Zahlen 1, 2, 3 mit Wiederholung setzt, 10 verschiedene Gleichungen ergeben. Die Gleichung (17.) stellt also ein System von 10 Gleichungen mit 30 Multiplicatoren A und 10 Multiplicatoren p dar. Nimmt man nun an, dafs die gegebene Function ψ

$$= c_{1,1,1}x_1x_1x_1 + c_{2,2,2}x_2x_2x_2 + c_{3,3,3}x_3x_3x_3 + 3c_{1,1,2}x_1x_1x_2 + 3c_{1,1,3}x_1x_1x_3$$
$$+ 3c_{2,2,1}x_2x_2x_1 + 3c_{2,2,3}x_2x_2x_3 + 3c_{3,3,1}x_3x_3x_1 + 3c_{3,3,2}x_3x_3x_2 + 6c_{1,2,3}x_1x_2x_3$$

sei, welcher Ausdruck kürzer durch $\Sigma c_{\varkappa,\lambda,\mu}\, x_\varkappa x_\lambda x_\mu$ bezeichnet werden kann, da man aus dem Gliede $c_{\varkappa,\lambda,\mu}\, x_\varkappa x_\lambda x_\mu$ die ganze Summe erhält, wenn man für $\varkappa$, λ, μ

nach einander die Combinationen der Zahlen 1, 2, 3 mit Wiederholung und ihre Permutationen setzt und addirt, auch wie oben annimmt, dafs $c_{\varkappa,\lambda,\mu} = c_{\varkappa,\mu,\lambda} = \ldots$ sei: so kann man die Multiplicatoren in der Gleichung (16.) durch die 40 Multiplicatoren in dem Systeme von Gleichungen (17.) auf folgende Art ausdrücken:

$$18. \quad \begin{cases} p = \Sigma c_{\varkappa,\lambda,\mu} \cdot p_{\varkappa,\lambda,\mu}, & A^{(2)} = \Sigma c_{\varkappa,\lambda,\mu} \cdot A^{(2)}_{\varkappa,\lambda,\mu}, \\ A^{(1)} = \Sigma c_{\varkappa,\lambda,\mu} \cdot A^{(1)}_{\varkappa,\lambda,\mu}, & A^{(3)} = \Sigma c_{\varkappa,\lambda,\mu} \cdot A^{(3)}_{\varkappa,\lambda,\mu}. \end{cases}$$

9) Es bleiben noch die 40 Multiplicatoren des durch (17.) dargestellten Systems von Gleichungen zu bestimmen übrig. Da hierzu die Kenntnifs der gegebenen Functionen erforderlich ist, so nehme man an, es sei

$$19. \quad \begin{cases} f_1 = \Sigma a^{(1)}_{\varkappa,\lambda} x_\varkappa x_\lambda, \quad f_2 = \Sigma a^{(2)}_{\varkappa,\lambda} x_\varkappa x_\lambda, \quad f_3 = \Sigma a^{(3)}_{\varkappa,\lambda} x_\varkappa x_\lambda, \\ \varphi = \Sigma b_{\varkappa,\lambda,\mu} x_\varkappa x_\lambda x_\mu, \end{cases}$$

wo $a^{(\mu)}_{\varkappa,\lambda} = a^{\mu}_{\lambda,\varkappa}$ und für $\varkappa$, λ die Combinationen der Zahlen 1, 2, 3 zu zweien mit Wiederholung und ihre Permutationen zu setzen sind. Multiplicirt man nun die Gleichung (17.) mit dem unbestimmten Factor $\pi_{\varkappa,\lambda,\mu}$ und bildet ein System von Gleichungen, indem man für $\varkappa$, λ, μ alle Combinationen der Zahlen 1, 2, 3 mit Wiederholung und die Permutationen derselben setzt, so erhält man durch Addition:

$$20. \quad \varphi \Sigma p_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} + f_1 \Sigma A^{(1)}_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} + f_2 \Sigma A^{(2)}_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} + f_3 \Sigma A^{(3)}_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} = R \Sigma \pi_{\varkappa,\lambda,\mu} x_\varkappa x_\lambda x_\mu.$$

Die 10 unbestimmten Factoren π lassen sich aber so bestimmen, dafs den drei Gleichungen

$$\Sigma A^{(1)}_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} = 0; \quad \Sigma A^{(2)}_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} = 0; \quad \Sigma A^{(3)}_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} = 0$$

Genüge geschieht, worauf die Gleichung (20.) in

$$\varphi \Sigma p_{\varkappa,\lambda,\mu} \pi_{\varkappa,\lambda,\mu} = R \Sigma \pi_{\varkappa,\lambda,\mu} x_\varkappa x_\lambda x_\mu$$

übergeht. Jede der drei ersten Gleichungen zerfällt, da die Gröfsen A lineäre und homogene Functionen der Variabeln sind, von welchen die Bestimmung der Factoren π unabhängig sein mufs, in drei andere, so dafs man zur Bestimmung der 10 Factoren π nur 9 Gleichungen hat. Bemerkt man nun, dafs die letzte Gleichung unabhängig von den besondern Werthen der Variabeln stattfindet, so folgt hieraus, dafs die Gröfsen b den entsprechenden Gröfsen π proportional sind. Setzt man daher einen der Factoren π, z. B. $\pi_{1,1,1}$, der willkürlich bestimmt werden kann, gleich $b_{1,1,1}$, so werden auch die übrigen Gröfsen π den mit gleichen Indices behafteten Gröfsen b gleich sein. Dieses

10 *

vorausgesetzt, so folgt aus der letzten Gleichung und den drei vorhergehenden:

$$21.\quad \begin{cases} R = \Sigma p_{\varkappa,\lambda,\mu}\, b_{\varkappa,\lambda,\mu}, \\ \Sigma A^{(1)}_{\varkappa,\lambda,\mu}\, b_{\varkappa,\lambda,\mu} = 0, \quad \Sigma A^{(2)}_{\varkappa,\lambda,\mu}\, b_{\varkappa,\lambda,\mu} = 0, \quad \Sigma A^{(3)}_{\varkappa,\lambda,\mu}\, b_{\varkappa,\lambda,\mu} = 0. \end{cases}$$

Man kann die 10 Factoren π aber auch bestimmen, indem man mit ν irgend eine der Zahlen 1, 2, 3 bezeichnet, nemlich aus den Gleichungen

$$\Sigma p_{\varkappa,\lambda,\mu}\pi_{\varkappa,\lambda,\mu} = 0, \qquad \Sigma A^{(1)}_{\varkappa,\lambda,\mu}\pi_{\varkappa,\lambda,\mu} = Rx_\nu,$$
$$\Sigma A^{(2)}_{\varkappa,\lambda,\mu}\pi_{\varkappa,\lambda,\mu} = 0, \qquad \Sigma A^{(3)}_{\varkappa,\lambda,\mu}\pi_{\varkappa,\lambda,\mu} = 0,$$

von denen jede, mit Ausnahme der ersten, in drei andere zerfällt. Mit Rücksicht auf diese Gleichungen geht die Gleichung (20.) in

$$f_1 Rx_\nu = R\Sigma\pi_{\varkappa,\lambda,\mu}\, x_\varkappa x_\lambda x_\mu \quad \text{oder in} \quad f_1 x_\nu = \Sigma\pi_{\varkappa,\lambda,\mu}\, x_\varkappa x_\lambda x_\mu$$

über, woraus man durch Gleichsetzung der Coëfficienten gleicher Potenzen und Producte der Variabeln auf beiden Seiten der Gleichung die gesuchten Werthe der Factoren π erhält. Setzt man diese Werthe der Factoren π in die obigen 4 Gleichungen, so erhält man

$$22.\quad \begin{cases} \Sigma p_{\varkappa,\lambda,\nu}\, a^{(1)}_{\varkappa,\lambda} = 0, \\ \Sigma A^{(1)}_{\varkappa,\lambda,\nu}\, a^{(1)}_{\varkappa,\lambda} = Rx_\nu, \quad \Sigma A^{(2)}_{\varkappa,\lambda,\nu}\, a^{(1)}_{\varkappa,\lambda} = 0, \quad \Sigma A^{(3)}_{\varkappa,\lambda,\nu}\, a^{(1)}_{\varkappa,\lambda} = 0; \end{cases}$$

wobei zu beachten ist, dafs die Summenzeichen sich nur auf die verschiedenen Werthe der Indices $\varkappa$, λ, für welche man die Combinationen der Zahlen 1, 2, 3 zu zweien mit Wiederholung und deren Permutationen zu setzen hat, aber nicht auf die verschiedenen Werthe von ν beziehen; welches auch für die folgenden Gleichungen (23.) und (24.) gilt.

Aus den Gleichungen (22.) erhält man ein neues System, wenn man für die oberen Indices (1.), (2.), (3.) respective (2.), (3.), (1.) setzt, nemlich:

$$23.\quad \begin{cases} \Sigma p_{\varkappa,\lambda,\nu}\, a^{(2)}_{\varkappa,\lambda} = 0, \\ \Sigma A^{(1)}_{\varkappa,\lambda,\nu}\, a^{(2)}_{\varkappa,\lambda} = 0, \quad \Sigma A^{(2)}_{\varkappa,\lambda,\nu}\, a^{(2)}_{\varkappa,\lambda} = Rx_\nu, \quad \Sigma A^{(3)}_{\varkappa,\lambda,\nu}\, a^{(2)}_{\varkappa,\lambda} = 0; \end{cases}$$

woraus endlich durch dieselbe Veränderung der oberen Indices folgende Gleichungen entstehen:

$$24.\quad \begin{cases} \Sigma p_{\varkappa,\lambda,\mu}\, a^{(3)}_{\varkappa,\lambda} = 0, \\ \Sigma A^{(1)}_{\varkappa,\lambda,\nu}\, a^{(3)}_{\varkappa,\lambda} = 0, \quad \Sigma A^{(2)}_{\varkappa,\lambda,\nu}\, a^{(3)}_{\varkappa,\lambda} = 0, \quad \Sigma A^{(3)}_{\varkappa,\lambda,\nu}\, a^{(3)}_{\varkappa,\lambda} = Rx_\nu; \end{cases}$$

welche beiden Systeme auf gleiche Weise wie das System (22.) aus (20.) hätten abgeleitet werden können.

Die Gleichungen (21. bis 24.) enthalten alle Elemente zur Bestimmung der 40 Multiplicatoren p und A, welche in dem durch (17.) dargestellten Systeme enthalten sind. Denn da aus jeder der Gleichungen (22. bis 24.)

drei hervorgehen, indem man für ν nacheinander die Zahlen 1, 2, 3 setzt, so hat man, wenn man die Gleichungen (21.) hinzurechnet, im Ganzen 40 Gleichungen, in welche die zu bestimmenden Multiplicatoren auf lineäre Weise eingehen.

10) Da von den 40 Multiplicatoren p und A nur die 10 Multiplicatoren p in der folgenden Untersuchung eine Rolle spielen, so genügt es, die Gleichungen zusammenzustellen, deren Auflösung die Werthe dieser Multiplicatoren giebt. Sie sind folgende:

$$(25.)\qquad R = \Sigma p_{\varkappa,\lambda,\mu}.b_{\varkappa,\lambda,\mu};$$

$$26.\quad \begin{cases} 0 = \Sigma p_{\varkappa,\lambda,1} a^{(1)}_{\varkappa,\lambda}; & 0 = \Sigma p_{\varkappa,\lambda,1} a^{(2)}_{\varkappa,\lambda}; & 0 = \Sigma p_{\varkappa,\lambda,1} a^{(3)}_{\varkappa,\lambda}; \\ 0 = \Sigma p_{\varkappa,\lambda,2} a^{(1)}_{\varkappa,\lambda}; & 0 = \Sigma p_{\varkappa,\lambda,2} a^{(2)}_{\varkappa,\lambda}; & 0 = \Sigma p_{\varkappa,\lambda,2} a^{(3)}_{\varkappa,\lambda}; \\ 0 = \Sigma p_{\varkappa,\lambda,3} a^{(1)}_{\varkappa,\lambda}; & 0 = \Sigma p_{\varkappa,\lambda,3} a^{(2)}_{\varkappa,\lambda}; & 0 = \Sigma p_{\varkappa,\lambda,3} a^{(3)}_{\varkappa,\lambda}; \end{cases}$$

woraus sich R als die Determinante der Coëfficienten der Gröfsen p ergiebt.

Nimmt man an, dafs die Functionen f_1, f_2, f_3 für die Werthe der Variabeln $x_1 = x$, $x_2 = y$, $x_3 = 1$ verschwinden, dafs also die drei Gleichungen $f_1(x, y, 1) = 0$, $f_2(x, y, 1) = 0$, $f_3(x, y, 1) = 0$ stattfinden, so geht die Gleichung (27.) in

$$p_{\varkappa,\lambda,\mu}\varphi = R x_\varkappa x_\lambda x_\mu$$

über, woraus für die genannten Werthe der Variabeln die Proportion

$$x_1x_1x_1 : x_2x_2x_2 : x_3x_3x_3 : x_1x_1x_2 : \ldots\ldots : x_1x_2x_3 =$$
$$p_{1,1,1} : p_{2,2,2} : p_{3,3,3} : p_{1,1,2} : \ldots\ldots : p_{1,2,3}$$

folgt. In der That sind auch die Verhältnisse der Gröfsen p von der Function φ unabhängig; was schon in No. 8. bemerkt wurde und auch aus der Gleichung (26.) zu entnehmen ist. Beiläufig mag bemerkt werden, dafs die Verhältnisse der Gröfsen p unbestimmt werden müssen, wenn den drei Gleichungen noch ein zweites Werthenpaar x, y genügt. Nimmt man ferner an, dafs φ eine Function sei, welche für die Werthe $x_1 = x$, $x_2 = y$, $x_3 = 1$ ebenfalls verschwindet, so mufs auch R verschwinden. Es wird also unter dieser Annahme $R = 0$ zu dem Resultat der Elimination der Variabeln x, y aus den drei Gleichungen $f_1(x, y, 1) = 0$, $f_2(x, y, 1) = 0$, $f_3(x, y, 1) = 0$. Demnach ist es für die Elimination der Variabeln aus drei gegebenen Gleichungen vom zweiten Grade wichtig, eine passende Function vom dritten Grade zu haben, welche für dasjenige Werthenpaar verschwindet, so den drei gegebenen Gleichungen genügt. Eine solche Function soll in der folgenden Nummer näher untersucht werden.

11) Die drei Functionen f_1, f_2, f_3 kann man, wenn man der Kürze wegen $u^{(\lambda)}_\varkappa$ statt $\frac{df}{dx_\lambda}$ setzt, weil sie homogen und vom zweiten Grade sind,

so darstellen:

$$27.\quad \begin{cases} x_1 u_1^{(1)} + x_2 u_1^{(2)} + x_3 u_1^{(3)} = 2f_1, \\ x_1 u_2^{(1)} + x_2 u_2^{(2)} + x_3 u_2^{(3)} = 2f_2, \\ x_1 u_3^{(1)} + x_2 u_3^{(2)} + x_3 u_3^{(3)} = 2f_3. \end{cases}$$

Betrachtet man die in diesen Gleichungen explicite und lineär vorkommenden Variabeln x_1, x_2, x_3 als die Unbekannten und löset die Gleichungen nach ihnen auf, so stellen sich die Werthe derselben als Brüche dar, mit gleichen Nennern. Dieser gemeinschaftliche Nenner, der mit dem Namen der *Determinante* der Functionen f_1, f_2, f_3 bezeichnet zu werden pflegt, und welcher in dem vorliegenden Falle in Rücksicht auf die in ihm enthaltenen Variabeln vom dritten Grade ist, soll von jetzt an mit dem Zeichen φ bezeichnet werden, unter welchem Zeichen bis dahin eine beliebige Function vom dritten Grade zwischen den Variabeln x_1, x_2, x_3 verstanden wurde. Dieses vorausgesetzt, ist:

$$28.\quad \varphi = u_1^{(1)}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + u_2^{(1)}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} + u_3^{(1)}\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\}$$

und wenn man auf die angegebene Art die Gleichungen (27.) auflöset, so erhält man:

$$29.\quad \begin{cases} x_1\varphi = 2f_1\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + 2f_2\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} + 2f_3\{u_1^{(2)}u_2^{(3)} - u_1^{(2)}u_2^{(3)}\}, \\ x_2\varphi = 2f_1\{u_2^{(3)}u_3^{(1)} - u_2^{(1)}u_3^{(3)}\} + 2f_2\{u_3^{(3)}u_1^{(1)} - u_3^{(1)}u_1^{(3)}\} + 2f_3\{u_1^{(3)}u_2^{(1)} - u_1^{(1)}u_2^{(3)}\}, \\ x_3\varphi = 2f_1\{u_2^{(1)}u_3^{(2)} - u_2^{(2)}u_3^{(1)}\} + 2f_2\{u_3^{(1)}u_1^{(2)} - u_3^{(2)}u_1^{(1)}\} + 2f_3\{u_1^{(1)}u_2^{(2)} - u_1^{(2)}u_2^{(1)}\}; \end{cases}$$

woraus folgt:

Lehrsatz 2.

Wenn drei homogene Functionen zweiten Grades von drei Variabeln für ein System von Werthen dieser Variabeln verschwinden, so verschwindet auch die Determinante dieser Functionen für dasselbe System von Werthen.

Dieser Lehrsatz gilt nicht allein für drei homogene Functionen vom 2ten Grade von 3 Variabeln, sondern auch für eine beliebige Zahl von homogenen Functionen irgend welcher Grade mit einer gleichen Zahl Variabeln.

Durch partielle Differentiation der ersten Gleichung (29.) nach den Variablen x_1 oder x_2 erhält man, wenn man der Kürze wegen durch φ_λ die Differentiation der Determinante φ, nach x_λ genommen, andeutet:

$$x_1\varphi_1 + \varphi =$$
$$2[u_1^{(1)}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + u_2^{(1)}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} + u_3^{(1)}\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\}]$$
$$+ 2f_1\frac{d}{dx_1}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + 2f_2\frac{d}{dx_1}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} + 2f_3\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\},$$

$$x_1\varphi_2 =$$
$$2\,[u_1^{(2)}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + u_2^{(2)}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} + u_3^{(2)}\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\}]$$
$$+ 2f_1\frac{d}{dx_2}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + 2f_2\frac{d}{dx_2}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} + 2f_3\frac{d}{dx_2}\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\}.$$

Es ist leicht zu bemerken, dafs in der ersten Gleichung der erste Theil rechts vom Gleichheitszeichen nach (28.) gleich 2φ ist, und dafs in der zweiten Gleichung der entsprechende Theil von selbst verschwindet. Berücksichtigt man dieses, so stellen sich die differenzïirten Gleichungen (29.) wie folgt dar:

$$30.\quad \begin{cases}
x_1\varphi_1 - \varphi = 2f_1\frac{d}{dx_1}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + 2f_2\frac{d}{dx_1}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} \\
\qquad + 2f_3\frac{d}{dx_1}\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\}, \\
x_1\varphi_2 = 2f_1\frac{d}{dx_2}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + 2f_2\frac{d}{dx_2}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} \\
\qquad + 2f_3\frac{d}{dx_2}\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\}, \\
x_1\varphi_3 = 2f_1\frac{d}{dx_3}\{u_2^{(2)}u_3^{(3)} - u_2^{(3)}u_3^{(2)}\} + 2f_2\frac{d}{dx_3}\{u_3^{(2)}u_1^{(3)} - u_3^{(3)}u_1^{(2)}\} \\
\qquad + 2f_3\frac{d}{dx_3}\{u_1^{(2)}u_2^{(3)} - u_1^{(3)}u_2^{(2)}\}, \\
x_2\varphi_1 = 2f_1\frac{d}{dx_1}\{u_2^{(3)}u_3^{(1)} - u_2^{(1)}u_3^{(3)}\} + 2f_2\frac{d}{dx_1}\{u_3^{(3)}u_1^{(1)} - u_3^{(1)}u_1^{(3)}\} \\
\qquad + 2f_3\frac{d}{dx_1}\{u_1^{(3)}u_2^{(1)} - u_1^{(1)}u_2^{(3)}\}, \\
x_2\varphi_2 - \varphi = 2f_1\frac{d}{dx_2}\{u_2^{(3)}u_3^{(1)} - u_2^{(1)}u_3^{(3)}\} + 2f_2\frac{d}{dx_2}\{u_3^{(3)}u_1^{(1)} - u_3^{(1)}u_1^{(3)}\} \\
\qquad + 2f_3\frac{d}{dx_2}\{u_1^{(3)}u_2^{(1)} - u_1^{(1)}u_2^{(3)}\}, \\
x_2\varphi_3 = 2f_1\frac{d}{dx_3}\{u_2^{(3)}u_3^{(1)} - u_2^{(1)}u_3^{(3)}\} + 2f_2\frac{d}{dx_3}\{u_3^{(3)}u_1^{(1)} - u_3^{(1)}u_1^{(3)}\} \\
\qquad + 2f_3\frac{d}{dx_3}\{u_1^{(3)}u_2^{(1)} - u_1^{(1)}u_2^{(3)}\}, \\
x_3\varphi_1 = 2f_1\frac{d}{dx_1}\{u_2^{(1)}u_3^{(2)} - u_2^{(2)}u_3^{(1)}\} + 2f_2\frac{d}{dx_1}\{u_3^{(1)}u_1^{(2)} - u_3^{(2)}u_1^{(1)}\} \\
\qquad + 2f_3\frac{d}{dx_1}\{u_1^{(1)}u_2^{(2)} - u_1^{(2)}u_2^{(1)}\}, \\
x_3\varphi_2 = 2f_1\frac{d}{dx_2}\{u_2^{(1)}u_3^{(2)} - u_2^{(2)}u_3^{(1)}\} + 2f_2\frac{d}{dx_2}\{u_3^{(1)}u_1^{(2)} - u_3^{(2)}u_1^{(1)}\} \\
\qquad + 2f_3\frac{d}{dx_2}\{u_1^{(1)}u_2^{(2)} - u_1^{(2)}u_2^{(1)}\}, \\
x_3\varphi_3 - \varphi = 2f_1\frac{d}{dx_3}\{u_2^{(1)}u_3^{(2)} - u_2^{(2)}u_3^{(1)}\} + 2f_2\frac{d}{dx_3}\{u_3^{(1)}u_1^{(2)} - u_3^{(2)}u_1^{(1)}\} \\
\qquad + 2f_3\frac{d}{dx_3}\{u_1^{(1)}u_2^{(2)} - u_1^{(2)}u_2^{(1)}\}.
\end{cases}$$

Diese Gleichungen geben folgenden

Lehrsatz 3.

Wenn drei homogene Functionen zweiten Grades von drei Variabeln für ein System von Werthen dieser Variabeln verschwinden, so verschwinden auch die partiellen Differentialquotienten der Determinante dieser Functionen, nach den Variabeln genommen, für dasselbe System von Werthen.

Dieser Lehrsatz gilt allgemein für eine beliebige Zahl homogener Functionen mit einer gleichen Zahl von Variabeln, wenn die Functionen sämmtlich von einem und demselben Grade sind.

12) Die Coëfficienten der Entwicklung der Determinante φ nach den Potenzen und Producten der Variabeln wollen wir mit $b_{x,\lambda,\mu}$, in der Art bezeichnen, wie es in (19.) geschehen ist. Dieses vorausgesetzt, so ist die Bemerkung zu machen, *dafs φ in R übergeht, wenn man φ nach Potenzen und Producten der Variabeln entwickelt und für jedes Product $x_x x_\lambda x_\mu$ der Entwicklung $p_{x,\lambda,\mu}$* setzt. Dieses lehrt die Gleichung (25.). Zweitens bemerke man, *dafs, wenn man irgend eine der Functionen f_1, f_2, f_3, mit einer der Variabeln x_1, x_2, x_3 multiplicirt, nach Potenzen und Producten der Variabeln entwickelt, und $p_{x,\lambda,\mu}$ für jedes Product $x_x x_\lambda x_\mu$ setzt, der dadurch erhaltene Ausdruck verschwindet.* Dieses ergiebt sich aus der Ansicht der Gleichungen (26.).

Entwickelt man nun die identischen Gleichungen (30.) nach Potenzen und Producten der Variabeln und setzt für jedes Product $x_x x_\lambda x_\mu$ das entsprechende $p_{x,\lambda,\mu}$, so verschwinden, nach der zweiten Bemerkung, die Glieder rechts von den Gleichheitszeichen und man erhält:

$$31.\quad \begin{cases} \frac{1}{3}R = \Sigma p_{x,\lambda,1} b_{x,\lambda,1}; & 0 = \Sigma p_{x,\lambda,1} b_{x,\lambda,2}; & 0 = p_{x,\lambda,1} b_{x,\lambda,3}; \\ 0 = \Sigma p_{x,\lambda,2} b_{x,\lambda,1}; & \frac{1}{3}R = \Sigma p_{x,\lambda,2} b_{x,\lambda,2}; & 0 = p_{x,\lambda,2} b_{x,\lambda,3}; \\ 0 = \Sigma p_{x,\lambda,3} b_{x,\lambda,1}; & 0 = \Sigma p_{x,\lambda,3} b_{x,\lambda,2}; & \frac{1}{3}R = p_{x,\lambda,3} b_{x,\lambda,3}. \end{cases}$$

Diese Gleichungen beweisen, *dafs die Ausdrücke φ; $x_1\varphi_1$; $x_2\varphi_2$; $x_3\varphi_3$ in R übergehen, wenn man nach Potenzen und Producten der Variabeln entwickelt und für jedes Product $x_x x_\lambda x_\mu$ der Entwicklung $p_{x,\lambda,\mu}$ setzt; und dafs die 6 Ausdrücke $x_2\varphi_1$, $x_3\varphi_1$, $x_3\varphi_2$, $x_1\varphi_2$, $x_1\varphi_3$ und $x_2\varphi_3$ durch dieselbe Operation verschwinden.*

Von diesen Gleichungen, so wie von den Gleichungen (26.), wird im Folgenden häufig Gebrauch gemacht werden.

13) Es sind durch f_1, f_2, f_3, φ_1, φ_2, φ_3 im Vorhergehenden folgende Ausdrücke bezeichnet worden:

$$32.\quad \left\{\begin{aligned}
f_1 &= a^{(1)}_{1,1}x_1x_1 + a^{(1)}_{2,2}x_2x_2 + a^{(1)}_{3,3}x_3x_3 + 2a^{(1)}_{2,3}x_2x_3 + 2a^{(1)}_{3,1}x_3x_1 + 2a^{(1)}_{1,2}x_1x_2,\\
f_2 &= a^{(2)}_{1,1}x_1x_1 + a^{(2)}_{2,2}x_2x_2 + a^{(2)}_{3,3}x_3x_3 + 2a^{(2)}_{2,3}x_2x_3 + 2a^{(2)}_{3,1}x_3x_1 + 2a^{(2)}_{1,2}x_1x_2,\\
f_3 &= a^{(3)}_{1,1}x_1x_1 + a^{(3)}_{2,2}x_2x_2 + a^{(3)}_{3,3}x_3x_3 + 2a^{(3)}_{2,3}x_2x_3 + 2a^{(3)}_{3,1}x_3x_1 + 2a^{(3)}_{1,2}x_1x_2,\\
\tfrac{1}{3}\varphi_1 &= b_{1,1,1}x_1x_1 + b_{2,2,1}x_2x_2 + b_{3,3,1}x_3x_3 + 2b_{2,3,1}x_2x_3 + 2b_{3,1,1}x_3x_1 + 2b_{1,2,1}x_1x_2,\\
\tfrac{1}{3}\varphi_2 &= b_{1,1,2}x_1x_1 + b_{2,2,2}x_2x_2 + b_{3,3,2}x_3x_3 + 2b_{2,3,2}x_2x_3 + 2b_{3,1,2}x_3x_1 + 2b_{1,2,2}x_1x_2,\\
\tfrac{1}{3}\varphi_3 &= b_{1,1,3}x_1x_1 + b_{2,2,3}x_2x_2 + b_{3,3,3}x_3x_3 + 2b_{2,3,3}x_2x_3 + 2b_{3,1,3}x_3x_1 + 2b_{1,2,3}x_1x_2.
\end{aligned}\right.$$

Betrachtet man in diesen Gleichungen die 6 Producte x_1x_1, x_2x_2, ... x_1x_2 als 6 Unbekannte, so erhält man durch Auflösung der Gleichungen nach diesen Unbekannten:

$$33.\quad \left\{\begin{aligned}
Rx_1x_1 &= q^{(1)}_{1,1}f_1 + q^{(2)}_{1,1}f_2 + q^{(3)}_{1,1}f_3 + p_{1,1,1}\varphi_1 + p_{1,1,2}\varphi_2 + p_{1,1,3}\varphi_3,\\
Rx_2x_2 &= q^{(1)}_{2,2}f_1 + q^{(2)}_{2,2}f_2 + q^{(3)}_{2,2}f_3 + p_{2,2,1}\varphi_1 + p_{2,2,2}\varphi_2 + p_{2,2,3}\varphi_3,\\
Rx_3x_3 &= q^{(1)}_{3,3}f_1 + q^{(2)}_{3,3}f_2 + q^{(3)}_{3,3}f_3 + p_{3,3,1}\varphi_1 + p_{3,3,2}\varphi_2 + p_{3,3,3}\varphi_3,\\
Rx_2x_3 &= q^{(1)}_{2,3}f_1 + q^{(2)}_{2,3}f_2 + q^{(3)}_{2,3}f_3 + p_{2,3,1}\varphi_1 + p_{2,3,2}\varphi_2 + p_{2,3,3}\varphi_3,\\
Rx_3x_1 &= q^{(1)}_{3,1}f_1 + q^{(2)}_{3,1}f_2 + q^{(3)}_{3,1}f_3 + p_{3,1,1}\varphi_1 + p_{3,1,2}\varphi_2 + p_{3,1,3}\varphi_3,\\
Rx_1x_2 &= q^{(1)}_{1,2}f_1 + q^{(2)}_{1,2}f_2 + q^{(3)}_{1,2}f_3 + p_{1,2,1}\varphi_1 + p_{1,2,2}\varphi_2 + p_{1,2,3}\varphi_3.
\end{aligned}\right.$$

Denn setzt man die Werthe der Unbekannten aus (33.) in (32.), so erhält man durch Gleichsetzung der Coëfficienten von φ_1, φ_2, φ_3 die Gleichungen (26.) und (31.), und durch Gleichsetzung der Coëfficienten von f_1, f_2, f_3 auf beiden Seiten der Gleichungen folgende Gleichungen

$$34.\quad \left\{\begin{aligned}
&R = \Sigma q^{(1)}_{\varkappa,\lambda}.a^{(1)}_{\varkappa,\lambda}; && 0 = \Sigma q^{(1)}_{\varkappa,\lambda}.a^{(2)}_{\varkappa,\lambda}; && 0 = \Sigma q^{(1)}_{\varkappa,\lambda}.a^{(3)}_{\varkappa,\lambda};\\
&0 = \Sigma q^{(2)}_{\varkappa,\lambda}.a^{(1)}_{\varkappa,\lambda}; && R = \Sigma q^{(2)}_{\varkappa,\lambda}.a^{(2)}_{\varkappa,\lambda}; && 0 = \Sigma q^{(2)}_{\varkappa,\lambda}.a^{(3)}_{\varkappa,\lambda};\\
&0 = \Sigma q^{(3)}_{\varkappa,\lambda}.a^{(1)}_{\varkappa,\lambda}; && 0 = \Sigma q^{(3)}_{\varkappa,\lambda}.a^{(2)}_{\varkappa,\lambda}; && R = \Sigma q^{(3)}_{\varkappa,\lambda}.a^{(3)}_{\varkappa,\lambda};
\end{aligned}\right.$$

$$35.\quad \left\{\begin{aligned}
&0 = \Sigma q^{(1)}_{\varkappa,\lambda}b_{\varkappa,\lambda,1}; && 0 = \Sigma q^{(1)}_{\varkappa,\lambda}b_{\varkappa,\lambda,2}; && 0 = \Sigma q^{(1)}_{\varkappa,\lambda}b_{\varkappa,\lambda,3};\\
&0 = \Sigma q^{(2)}_{\varkappa,\lambda}b_{\varkappa,\lambda,1}; && 0 = \Sigma q^{(2)}_{\varkappa,\lambda}b_{\varkappa,\lambda,2}; && 0 = \Sigma q^{(2)}_{\varkappa,\lambda}b_{\varkappa,\lambda,3};\\
&0 = \Sigma q^{(3)}_{\varkappa,\lambda}b_{\varkappa,\lambda,1}; && 0 = \Sigma q^{(3)}_{\varkappa,\lambda}b_{\varkappa,\lambda,2}; && 0 = \Sigma q^{(3)}_{\varkappa,\lambda}b_{\varkappa,\lambda,3}.
\end{aligned}\right.$$

Diese beiden Systeme Gleichungen dienen zur Bestimmung der 18 Coëfficienten q. Was die Coëfficienten p der Gleichungen (33.) betrifft, so beträgt die Zahl der von einander verschiedenen nur 10; wegen welchen Umstandes eben die Gleichungen (32.) und ihre Auflösungen (33.) merkwürdig sind.

14) Nimmt man an, dafs für ein System Werthe der Variabeln $x_1 = x$, $x_2 = y$, $x_3 = 1$ die Functionen f_1, f_2, f_3 verschwinden, so folgt aus dem Lehrsatze (3.), dafs für dasselbe System Werthe auch φ_1, φ_2, φ_3 verschwin-

den, und aus (33.), dafs R verschwindet. Es ist demnach $R=0$ das Resultat der Elimination der Variabeln aus den drei Gleichungen $f_1(x, y, 1)=0$, $f_2(x, y, 1)=0$, $f_3(x, y, 1)=0$. Da aber R die Determinante der Coëfficienten der 6 Producte $x_1 x_1$, $x_2 x_2$, ... $x_1 x_2$ in den Gleichungen (32.), also in Rücksicht auf alle Coëfficienten homogen und vom 6ten Grade, in Rücksicht auf die Coëfficienten in den einzelnen Gleichungen aber lineär ist: so wird man, wenn man für die Coëfficienten b ihre Werthe setzt, welche in Rücksicht auf die Coëfficienten der drei ersten Gleichungen Ausdrücke vom 3ten Grade und in Rücksicht auf die Coëfficienten jeder einzelnen dieser Gleichungen lineäre Ausdrücke sind, die Gleichung $R=0$ in Rücksicht auf die Coëfficienten der drei Gleichungen $f_1(x, y, 1)=0$, $f_2(x, y, 1)=0$, $f_3(x, y, 1)=0$ homogen und vom 12ten Grade, und in Rücksicht auf die Coëfficienten jeder einzelnen Gleichung vom 4ten Grade finden. Die angegebenen Eigenschaften der Determinante R und der Gleichung $R=0$ ergeben sich ebenfalls aus der Zusammensetzung der Determinante aus den Coëfficienten der Gröfsen p in den Gleichungen (25.) und (26.). Dieses sind aber nach Lehrsatz 1. die Criterien für die Endgleichung, welche aus der Elimination der Variabeln aus den genannten drei Gleichungen hervorgeht. Demnach läfst sich die angedeutete Eliminationsmethode in Form eines Lehrsatzes wie folgt ausdrücken:

Lehrsatz 4.

Wenn drei Gleichungen vom dritten Grade $f_1(x, y)=0$, $f_2(x, y)=0$, $f_3(x, y)=0$ *zwischen den Variabeln* x, y *gegeben sind, so erhält man die aus der Elimination dieser Variabeln hervorgehende Endgleichung, wenn man die Determinante* φ *der Functionen*

$$x_3 x_3 f_1\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right), \quad x_3 x_3 f_2\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right), \quad x_3 x_3 f_3\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right)$$

zusammenstellt und aus den 6 Gleichungen

$$x_3 x_3 f_1\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right)=0, \quad x_3 x_3 f_2\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right)=0, \quad x_3 x_3 f_3\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right)=0,$$

$$\frac{\partial \varphi}{\partial x_1}=0, \qquad \frac{\partial \varphi}{\partial x_2}=0, \qquad \frac{\partial \varphi}{\partial x_3}=0$$

die 6 Producte $x_1 x_1$, $x_2 x_2$, ... $x_1 x_2$ *eliminirt, wie wenn sie die Unbekannten wären.*

Da die genannten Producte in die 6 Gleichungen nur lineär eingehen, so ist durch den vorhergehenden Lehrsatz die Elimination der Variabeln aus drei Gleichungen vom zweiten Grade auf die Elimination der Unbekannten aus

linearen Gleichungen, oder, was dasselbe ist, auf die Bildung der aus den Coëfficienten linearer Gleichungen zusammengesetzten Determinante zurückgeführt.

15) Bisher bedeuteten die Zeichen f_1, f_2, f_3 ganz beliebige homogene Functionen zweiten Grades von den Variabeln x_1, x_2, x_3, und φ die Determinante jener Functionen. Von nun an sollen mit denselben Zeichen die partiellen Differentialquotienten von der homogenen Function

$$f = \Sigma a_{\varkappa,\lambda,\mu} x_\varkappa x_\lambda x_\mu$$

dritten Grades, nach den Variabeln x_1, x_2, x_3 genommen, und mit φ die Determinante jener partiellen Differentialquotienten bezeichnet werden; welche Determinante wir der Kürze wegen die ***Determinante der Function f*** nennen wollen. Dieses vorausgesetzt, so gelten die in den vorhergehenden Nummern entwickelten Gleichungen, wenn man überall $3a_{\varkappa,\lambda,\mu}$ statt $a^{\mu}_{\varkappa,\lambda}$ setzt, wodurch das System (32.) übergeht in:

$$32.^* \begin{cases} \frac{1}{3}f_1 = a_{1,1,1}x_1x_1 + a_{2,2,1}x_2x_2 + a_{3,3,1}x_3x_3 + 2a_{2,3,1}x_2x_3 + 2a_{3,1,1}x_3x_1 + 2a_{1,2,1}x_1x_2, \\ \frac{1}{3}f_2 = a_{1,1,2}x_1x_1 + a_{2,2,2}x_2x_2 + a_{3,3,2}x_3x_3 + 2a_{2,3,2}x_2x_3 + 2a_{3,1,2}x_3x_1 + 2a_{1,2,2}x_1x_2, \\ \frac{1}{3}f_3 = a_{1,1,3}x_1x_1 + a_{2,2,3}x_2x_2 + a_{3,3,3}x_3x_3 + 2a_{2,3,3}x_2x_3 + 2a_{3,1,3}x_3x_1 + 2a_{1,2,3}x_1x_2, \\ \frac{1}{3}\varphi_1 = b_{1,1,1}x_1x_1 + b_{2,2,1}x_2x_2 + b_{3,3,1}x_3x_3 + 2b_{2,3,1}x_2x_3 + 2b_{3,1,1}x_3x_1 + 2b_{1,2,1}x_1x_2, \\ \frac{1}{3}\varphi_2 = b_{1,1,2}x_1x_1 + b_{2,2,2}x_2x_2 + b_{3,3,2}x_3x_3 + 2b_{2,3,2}x_2x_3 + 2b_{3,1,2}x_3x_1 + 2b_{1,2,2}x_1x_2, \\ \frac{1}{3}\varphi_3 = b_{1,1,3}x_1x_1 + b_{2,2,3}x_2x_2 + b_{3,3,3}x_3x_3 + 2b_{2,3,3}x_2x_3 + 2b_{3,1,1}x_3x_1 + 2b_{1,2,3}x_1x_2. \end{cases}$$

Löset man dieses in Rücksicht auf die 6 Producte x_1x_1, x_2x_2, ... x_1x_3 lineäre System von Gleichungen nach diesen Producten auf, als ob sie die Unbekannten wären, so erhält man die Gleichung (33.). Zur Bestimmung von R und der 18 Gröfsen q, welche letztere enthalten, dienen dann die Gleichungen (35.) und folgende:

$$34.^* \begin{cases} \frac{1}{3}R = \Sigma q^{(1)}_{\varkappa,\lambda} a_{\varkappa,\lambda,1}; & 0 = \Sigma q^{(1)}_{\varkappa,\lambda} a_{\varkappa,\lambda,2}; & 0 = \Sigma q^{(1)}_{\varkappa,\lambda} a_{\varkappa,\lambda,3}; \\ 0 = \Sigma q^{(2)}_{\varkappa,\lambda} a_{\varkappa,\lambda,1}; & \frac{1}{3}R = \Sigma q^{(2)}_{\varkappa,\lambda} a_{\varkappa,\lambda,2}; & 0 = \Sigma q^{(2)}_{\varkappa,\lambda} a_{\varkappa,\lambda,3}; \\ 0 = \Sigma q^{(3)}_{\varkappa,\lambda} a_{\varkappa,\lambda,1}; & 0 = \Sigma q^{(3)}_{\varkappa,\lambda} a_{\varkappa,\lambda,2}; & \frac{1}{3}R = \Sigma q^{(3)}_{\varkappa,\lambda} a_{\varkappa,\lambda,3}. \end{cases}$$

Zwischen den 10 Gröfsen p und R hat man die Relationen (31.) und

$$26.^* \begin{cases} 0 = \Sigma p_{\varkappa,\lambda,1} a_{\varkappa,\lambda,1}; & 0 = \Sigma p_{\varkappa,\lambda,1} a_{\varkappa,\lambda,2}; & 0 = \Sigma p_{\varkappa,\lambda,1} a_{\varkappa,\lambda,3}; \\ 0 = \Sigma p_{\varkappa,\lambda,2} a_{\varkappa,\lambda,1}; & 0 = \Sigma p_{\varkappa,\lambda,2} a_{\varkappa,\lambda,2}; & 0 = \Sigma p_{\varkappa,\lambda,2} a_{\varkappa,\lambda,3}; \\ 0 = \Sigma p_{\varkappa,\lambda,3} a_{\varkappa,\lambda,1}; & 0 = \Sigma p_{\varkappa,\lambda,3} a_{\varkappa,\lambda,2}; & 0 = \Sigma p_{\varkappa,\lambda,3} a_{\varkappa,\lambda,3}. \end{cases}$$

Nachdem man die Werthe von R und der 10 Gröfsen p gefunden, kann man sich die Aufgabe stellen: Die Werthe der Gröfsen b zu bestimmen, welche nur den Gleichungen (31.) genügen. Da die Zahl der zu bestimmenden Gröfsen b gleich 10, dagegen die Zahl der bestimmenden Gleichungen 9

ist, so werden die gesuchten Gröfsen sämmtlich eine willkürliche Constante enthalten. Bezeichnet man diese willkürliche Constante mit m, so wird der allgemeine Ausdruck der gesuchten Gröfsen, welcher, für $b_{\varkappa,\lambda,\mu}$ in (31.) gesetzt, diesen Gleichungen genügt,

$$b_{\varkappa,\lambda,\mu}+ma_{\varkappa,\lambda,\mu}$$

sein; was aus (26.) und (31.) erhellet. Hieraus folgt: *dafs jede homogene Function $\psi=\Sigma c_{\varkappa,\lambda,\mu}x_\varkappa x_\lambda x_\mu$ dritten Grades von den Variabeln x_1, x_2, x_3, deren Coëfficienten c statt b in die Gleichungen* (31.) *gesetzt diesen Gleichungen genügen, von der Form $\psi=\varphi+mf$ oder, wenn man in der Gleichung* (31.) *R eine beliebige Gröfse bedeuten läfst, von der Form $\psi=mf+n\varphi$ ist.* In der folgenden Nummer soll nachgewiesen werden, dafs die Determinante der Determinante von der Function f diese Eigenschaft hat.

16) Wenn man der Kürze wegen durch $v_\varkappa^{(\lambda)}$ den partiellen Differentialquotienten $\frac{\partial^2\varphi}{\partial x_\varkappa\partial x_\lambda}$ zweiter Ordnung bezeichnet, so ist

$$36.\quad\begin{cases}0=\frac{d}{dx_1}(v_2^{(2)}v_3^{(3)}-v_2^{(3)}v_3^{(2)})+\frac{d}{dx_2}(v_3^{(2)}v_1^{(3)}-v_3^{(3)}v_1^{(2)})+\frac{d}{dx_3}v_1^{(2)}v_2^{(3)}-v_1^{(3)}v_2^{(2)}),\\ 0=\frac{d}{dx_1}(v_2^{(3)}v_3^{(1)}-v_2^{(1)}v_3^{(3)})+\frac{d}{dx_2}(v_3^{(3)}v_1^{(1)}-v_3^{(1)}v_1^{(3)})+\frac{d}{dx_3}v_1^{(3)}v_2^{(1)}-v_1^{(1)}v_2^{(3)}),\\ 0=\frac{d}{dx_1}(v_2^{(1)}v_3^{(2)}-v_2^{(2)}v_3^{(1)})+\frac{d}{dx_2}(v_3^{(1)}v_1^{(2)}-v_3^{(2)}v_1^{(1)})+\frac{d}{dx_3}v_1^{(1)}v_2^{(2)}-v_1^{(2)}v_2^{(1)}).\end{cases}$$

Diese Gleichungen gelten auch allgemein für jede beliebige homogene Function φ 3ter Ordnung von drei Variabeln. Aus diesen identischen Gleichungen geht ein System von 9 Gleichungen durch Differentiation nach den drei Variabeln hervor, welches in der vorliegenden Untersuchung eine Anwendung finden wird.

Bezeichnet man ferner mit $\psi=\Sigma c_{\varkappa,\lambda,\mu}x_\varkappa x_\lambda x_\mu$ die Determinante der partiellen Differentialquotienten der Function φ, welche kürzer *die Determinante der Function* φ oder *die Determinante der Determinante der Function* f genannt wird; so ist klar, dafs, wenn man statt der Gröfsen a die entsprechenden Gröfsen b setzt, dadurch f in φ, φ in ψ, $f_\varkappa$ in $\varphi_\varkappa$, $\varphi_\varkappa$ in $\psi_\varkappa$ und $u_\varkappa^{(\lambda)}$, welches $=\frac{\partial_2 f}{\partial x_\varkappa\partial x_\lambda}$ ist, in $v_\varkappa^{(\lambda)}$ übergeht. Macht man diese Änderung in den Gleichungen (30.), entwickelt hierauf beide Seiten der Gleichungen nach Potenzen und Producten der Variabeln und setzt für jedes Product $x_\varkappa x_\lambda x_\mu$ der Entwicklung $p_{\varkappa,\lambda,\mu}$, so verschwinden, weil dadurch die Ausdrücke $x_1\varphi_1$, $x_2\varphi_2$, $x_3\varphi_3$ den Werth R und $x_2\varphi_1$, $x_3\varphi_1$, $x_3\varphi_2$, $x_1\varphi_2$, $x_1\varphi_3$, $x_2\varphi_3$ den Werth 0 annehmen, mit Rücksicht auf die durch Differentation der Gleichungen (36.)

abgeleiteten Gleichungen die Theile rechterhand der sämmtlichen Gleichungen und man erhält:

$$37. \begin{cases} \tfrac{1}{3}P = \Sigma p_{\varkappa,\lambda,1}c_{\varkappa,\lambda,1}, & 0 = \Sigma p_{\varkappa,\lambda,1}c_{\varkappa,\lambda,2}, & 0 = \Sigma p_{\varkappa,\lambda,1}c_{\varkappa,\lambda,3}, \\ 0 = \Sigma p_{\varkappa,\lambda,2}c_{\varkappa,\lambda,1}, & \tfrac{1}{3}P = \Sigma p_{\varkappa,\lambda,2}c_{\varkappa,\lambda,2}, & 0 = \Sigma p_{\varkappa,\lambda,2}c_{\varkappa,\lambda,3}, \\ 0 = \Sigma p_{\varkappa,\lambda,3}c_{\varkappa,\lambda,1}, & 0 = \Sigma p_{\varkappa,\lambda,3}c_{\varkappa,\lambda,2}, & \tfrac{1}{3}P = \Sigma p_{\varkappa,\lambda,3}c_{\varkappa,\lambda,3}, \end{cases}$$

$$P = \Sigma p_{\varkappa,\lambda,\mu}c_{\varkappa,\lambda,\mu}.$$

Diese Gleichungen beweisen, dafs die Gleichung (31.) erfüllt wird, wenn man c statt b setzt und statt R eine bestimmte andere Gröfse P; woraus denn nach der obigen Bemerkung folgt:

$$38. \quad c_{\varkappa,\lambda,\mu} = m a_{\varkappa,\lambda,\mu} + n b_{\varkappa,\lambda,\mu},$$

und dafs die Determinante ψ der Function φ von der Form

$$39. \quad \psi = mf + n\varphi$$

ist; was sich auf folgende Art ausdrücken läfst:

Lehrsatz 5.

Die Determinante der Determinante einer gegebenen homogenen Function dritten Grades von drei Variabeln ist gleich der Summe der gegebenen Function und ihrer Determinante, jede mit einem passenden constanten Factor multiplicirt.

Es ist noch zu bemerken, dafs

$$40. \quad P = nR$$

ist; welche Gleichung man erhält, wenn man die Werthe von $c_{\varkappa,\lambda,\mu}$ aus (38.) in (37.) setzt und die Gleichungen (26.*) und (31.) zu Hülfe nimmt.

17) Nimmt man an, dafs die Gröfsen $p_{\varkappa,\lambda,\mu}$ in $q_{\varkappa,\lambda,\mu}$ und R in S übergehen, wenn man für die Gröfsen a die entsprechenden Gröfsen b setzt, so gehen die Gleichungen (26.*) in

$$41. \begin{cases} 0 = \Sigma q_{\varkappa,\lambda,1}b_{\varkappa,\lambda,1}; & 0 = \Sigma q_{\varkappa,\lambda,1}b_{\varkappa,\lambda,2}; & 0 = \Sigma q_{\varkappa,\lambda,1}b_{\varkappa,\lambda,3}; \\ 0 = \Sigma q_{\varkappa,\lambda,2}b_{\varkappa,\lambda,1}; & 0 = \Sigma q_{\varkappa,\lambda,2}b_{\varkappa,\lambda,2}; & 0 = \Sigma q_{\varkappa,\lambda,2}b_{\varkappa,\lambda,3}; \\ 0 = \Sigma q_{\varkappa,\lambda,3}b_{\varkappa,\lambda,1}; & 0 = \Sigma q_{\varkappa,\lambda,3}b_{\varkappa,\lambda,2}; & 0 = \Sigma q_{\varkappa,\lambda,3}b_{\varkappa,\lambda,3} \end{cases}$$

über und man erhält aus (31.):

$$42. \begin{cases} \tfrac{1}{3}S = \Sigma q_{\varkappa,\lambda,1}c_{\varkappa,\lambda,1}; & 0 = \Sigma q_{\varkappa,\lambda,1}c_{\varkappa,\lambda,2}; & 0 = \Sigma q_{\varkappa,\lambda,1}c_{\varkappa,\lambda,3}; \\ 0 = \Sigma q_{\varkappa,\lambda,2}c_{\varkappa,\lambda,1}; & \tfrac{1}{3}S = \Sigma q_{\varkappa,\lambda,2}c_{\varkappa,\lambda,2}; & 0 = \Sigma q_{\varkappa,\lambda,2}c_{\varkappa,\lambda,3}; \\ 0 = \Sigma q_{\varkappa,\lambda,3}c_{\varkappa,\lambda,1}; & 0 = \Sigma q_{\varkappa,\lambda,3}c_{\varkappa,\lambda,2}; & \tfrac{1}{3}S = \Sigma q_{\varkappa,\lambda,3}c_{\varkappa,\lambda,3}. \end{cases}$$

Durch Substitution der Werthe von $c_{\varkappa,\lambda,\mu}$ aus (38.) in diesen Gleichungen erhält man, mit Rücksicht auf (41.):

$$43.\quad\begin{cases} \tfrac{1}{3}\varrho R = q_{\varkappa,\lambda,1}a_{\varkappa,\lambda,1}; & 0 = \Sigma q_{\varkappa,\lambda,1}a_{\varkappa,\lambda,2}; & 0 = \Sigma q_{\varkappa,\lambda,1}a_{\varkappa,\lambda,3}; \\ 0 = q_{\varkappa,\lambda,2}a_{\varkappa,\lambda,1}; & \tfrac{1}{3}\varrho R = \Sigma q_{\varkappa,\lambda,2}a_{\varkappa,\lambda,2}; & 0 = \Sigma q_{\varkappa,\lambda,2}a_{\varkappa,\lambda,3}; \\ 0 = q_{\varkappa,\lambda,3}a_{\varkappa,\lambda,1}; & 0 = \Sigma q_{\varkappa,\lambda,3}a_{\varkappa,\lambda,2}; & \tfrac{1}{3}\varrho R = \Sigma q_{\varkappa,\lambda,3}a_{\varkappa,\lambda,3}; \end{cases}$$

$$44.\quad m\varrho R = S.$$

Aus den Gleichungen (41.) ist ersichtlich, *dafs, wenn man die Function φ, oder die Producte einer der Functionen φ_1, φ_2, φ_3 und einer der Variabeln x_1, x_2, x_3, nach Potenzen und Producten der Variabeln entwickelt und $q_{\varkappa,\lambda,\mu}$ für jedes Product $x_\varkappa x_\lambda x_\mu$ setzt, die dadurch entstehenden Ausdrücke verschwinden.*

Eben so geht aus den Gleichungen (43.) hervor, *dafs die nach Potenzen und Producten der Variabeln entwickelten Ausdrücke f, $x_1 f_1$, $x_2 f_2$, $x_3 f_3$ den Werth ϱR annehmen, wenn man $q_{\varkappa,\lambda,\mu}$ für $x_\varkappa x_\lambda x_\mu$ setzt, und dafs auf gleiche Weise die 6 Ausdrücke $x_2\varphi_1$, $x_3\varphi_1$, $x_3\varphi_2$, $x_1\varphi_2$, $x_1\varphi_3$, $x_2\varphi_3$ verschwinden.*

Auf gleiche Weise, wie die Systeme (35.) und (34.*) die Gröfsen $q^\mu_{\varkappa,\lambda}$ bestimmen, ergeben sich aus (41.) und (43.) die Gröfsen der Werthe $\frac{1}{\varrho}q_{\varkappa,\lambda,\mu}$. Mit andern Worten: die beiden letzten Systeme erhält man aus den beiden ersten, wenn man $\frac{1}{\varrho}\cdot q_{\varkappa,\lambda,\mu}$ für $q^\mu_{\varkappa,\lambda}$ setzt, woraus

$$45.\quad q^\mu_{\varkappa,\lambda} = \frac{1}{\varrho}\cdot q_{\varkappa,\lambda,\mu}$$

folgt. Setzt man diese Werthe von $q^\mu_{\varkappa,\lambda}$ in (33.), so erhält man

$$33.^*\quad\begin{cases} Rx_1x_1 = \frac{1}{\varrho}q_{1,1,1}f_1 + \frac{1}{\varrho}q_{1,1,2}f_2 + \frac{1}{\varrho}q_{1,1,3}f_3 + p_{1,1,1}\varphi_1 + p_{1,1,2}\varphi_2 + p_{1,1,3}\varphi_3, \\ Rx_2x_2 = \frac{1}{\varrho}q_{2,2,1}f_1 + \frac{1}{\varrho}q_{2,2,2}f_2 + \frac{1}{\varrho}q_{2,2,3}f_3 + p_{2,2,1}\varphi_1 + p_{2,2,2}\varphi_2 + p_{2,2,3}\varphi_3, \\ Rx_3x_3 = \frac{1}{\varrho}q_{3,3,1}f_1 + \frac{1}{\varrho}q_{3,3,2}f_2 + \frac{1}{\varrho}q_{3,3,3}f_3 + p_{3,3,1}\varphi_1 + p_{3,3,2}\varphi_2 + p_{3,3,3}\varphi_3, \\ Rx_2x_3 = \frac{1}{\varrho}q_{2,3,1}f_1 + \frac{1}{\varrho}q_{2,3,2}f_2 + \frac{1}{\varrho}q_{2,3,3}f_3 + p_{2,3,1}\varphi_1 + p_{2,3,2}\varphi_2 + p_{2,3,3}\varphi_3, \\ Rx_3x_1 = \frac{1}{\varrho}q_{3,1,1}f_1 + \frac{1}{\varrho}q_{3,1,2}f_2 + \frac{1}{\varrho}q_{3,1,3}f_3 + p_{3,1,1}\varphi_1 + p_{3,1,2}\varphi_2 + p_{3,1,3}\varphi_3, \\ Rx_1x_2 = \frac{1}{\varrho}q_{1,2,1}f_1 + \frac{1}{\varrho}q_{1,2,2}f_2 + \frac{1}{\varrho}q_{1,2,3}f_3 + p_{1,2,1}\varphi_1 + p_{1,2,2}\varphi_2 + p_{1,2,3}\varphi_3. \end{cases}$$

Wenn man also in dem Systeme (32.) die 6 Producte x_1x_1, x_2x_2, ... x_1x_2 als die Unbekannten betrachtet, so erhält man durch Auflösung der Gleichungen nach diesen Unbekannten die Gleichungen* (33.*). Das Merkwürdige an diese Gleichungen besteht vorzüglich darin, dafs, während die

einen nur 20 verschiedene Coëfficienten a und b enthalten, die andern ebenfalls nur 20 verschiedene Coëfficienten p und $\frac{1}{\varrho}.q$ haben.

Wenn man in den Gleichungen (41.) und (43.), durch welche die Gröfsen $\frac{1}{\varrho}q_{x,\lambda,\mu}$ vollständig bestimmt sind, für $b_{x,\lambda,\mu}$ die Gröfsen $a_{x,\lambda,\mu}$ setzt, wodurch gleichzeitig $b_{x,\lambda,\mu}$ in $ma_{x,\lambda,\mu}+nb_{x,\lambda,\mu}$ und R in $S=m\varrho R$ übergehen, so werden die so geänderten Gleichungen erfüllt, wenn man $\frac{1}{\varrho}q_{x,\lambda,\mu}$ in $m\varrho p_{x,\lambda,\mu}-nq_{x,\lambda,\mu}$ verändert. Dieses beweiset, dafs durch die Veränderung von $a_{x,\lambda,\mu}$ in $b_{x,\lambda,\mu}$, $\frac{1}{\varrho}q_{x,\lambda,\mu}$ in $m\varrho p_{x,\lambda,\mu}-nq_{x,\lambda,\mu}$ übergeht.

Es bedeutet $\frac{R}{3^6}$ die aus den Coëfficienten der 6 Potenzen und Producte der Variabeln in Gleichung (32.*) gebildete Determinante. Diese geht in $\frac{S}{3^6}$ über, wenn man in ihr $b_{x,\lambda,\mu}$ für $a_{x,\lambda,\mu}$ und $ma_{x,\lambda,\mu}+nb_{x,\lambda,\mu}$ für $b_{x,\lambda,\mu}$ setzt. Ändert man daher die Coëfficienten in (32.*) auf die angegebene Art, und bildet hierauf aus den geänderten Coëfficienten die Determinante, so erhält man ebenfalls $\frac{S}{3^6}$. Dieselbe Gröfse erhält man aber auch, wenn man $a_{x,\lambda,\mu}$ in $b_{x,\lambda,\mu}$ und $b_{x,\lambda,\mu}$ in $ma_{x,\lambda,\mu}$ übergehen läfst und aus den so geänderten Coëfficienten die Determinante bildet. Diese wird aber $=\frac{m^3R}{3^6}$. Mithin ist $S=m^3R$; welcher Werth, in (44.) gesetzt,

$$46.\quad \varrho = m^2$$

giebt. Hieraus folgt nun, mit Rücksicht auf die obigen Bemerkungen, dafs

Wenn $a_{x,\lambda,\mu}$ in $b_{x,\lambda,\mu}$ übergeht, so geht gleichzeitig $b_{x,\lambda,\mu}$ in $ma_{x,\lambda,\mu}+nb_{x,\lambda,\mu}$, f in φ, f_x in φ_x, φ in $mf+n\varphi$, φ_x in $mf_x+n\varphi_x$, $p_{x,\lambda,\mu}$ in $q_{x,\lambda,\mu}$, $\frac{1}{\varrho}q_{x,\lambda,\mu}$ oder $\frac{1}{m^2}q_{x,\lambda,\mu}$ in $m^3p_{x,\lambda,\mu}-nq_{x,\lambda,\mu}$ und R in m^3R über.

18) Wenn man eine Function F aus einer gegebenen homogenen Function f vom 3ten Grade von den Variabeln x_1, x_2, x_3 und ihrer Determinante φ wie folgt zusammensetzt:

$$47.\quad F = d.f+\delta.\varphi,$$

wo d und δ beliebige Constanten bedeuten, und nun mit F_1, F_2, F_3 die partiellen Differentialquotienten der Function F nach den Variabeln genommen bezeichnet, so erhalten die Ausdrücke F, x_1F_1, x_2F_2, x_3F_3, wenn man sie nach Potenzen und Producten der Variabeln entwickelt und $p_{x,\lambda,\mu}$ für $x_x x_\lambda x_\mu$ setzt, die Werthe $\delta.R$; und auf gleiche Weise erhalten die Ausdrücke x_2F_1, x_3F_1, x_3F_2, x_1F_2, x_1F_3, x_2F_3 die Werthe 0. Eben so gehen die Ausdrücke F, x_1F_1, x_2F_2, x_3F_3, wenn man sie entwickelt und $\frac{1}{\varrho}q_{x,\lambda,\mu}$ für $x_x x_\lambda x_\mu$

setzt, in $d.R$ über, während die Ausdrücke x_2F_1, x_3F_1, x_3F_2, x_1F_2, x_1F_3, x_2F_3 verschwinden.

Die Determinante der Function F werde durch

$$48. \quad \Phi = \Sigma B_{x,\lambda,\mu} x_x x_\lambda x_\mu$$

bezeichnet; in welchem Ausdruck die Gröfsen $B_{x,\lambda,\mu}$ ganze homogene Functionen 3ter Ordnung in Rücksicht auf die Coëfficienten in F, also ganze homogene Functionen 3ter Ordnung in Rücksicht auf die Constanten d und δ sein werden. Bezeichnet man ferner mit Φ_1, Φ_2, Φ_3 die partiellen Differentialquotienten der Determinante Φ, nach den Variabeln genommen, und setzt der Kürze wegen $\frac{\partial^2 \Phi}{\partial x_x \partial x_\lambda} = v_x^{(\lambda)}$, so gelten die Gleichungen (36.) und (30.), wenn man in den letzteren f in F, φ in Φ und u in v verändert. Entwickelt man nun die auf diese Weise veränderten Gleichungen (30.) und setzt $p_{x,\lambda,\mu}$ für $x_x x_\lambda x_\mu$, so verschwinden, mit Berücksichtigung der durch Differentiation aus (36.) abgeleiteten 9 Gleichungen, die rechtseitigen Theile sämmtlicher Gleichungen und man erhält:

$$49. \begin{cases} \frac{1}{3}T = \Sigma p_{x,\lambda,1} B_{x,\lambda,1}; & 0 = \Sigma p_{x,\lambda,1} B_{x,\lambda,2}; & 0 = \Sigma p_{x,\lambda,1} B_{x,\lambda,3}; \\ 0 = \Sigma p_{x,\lambda,2} B_{x,\lambda,1}; & \frac{1}{3}T = \Sigma p_{x,\lambda,2} B_{x,\lambda,2}; & 0 = \Sigma p_{x,\lambda,2} B_{x,\lambda,3}; \\ 0 = \Sigma p_{x,\lambda,3} B_{x,\lambda,1}; & 0 = \Sigma p_{x,\lambda,3} B_{x,\lambda,2}; & \frac{1}{3}T = \Sigma p_{x,\lambda,3} B_{x,\lambda,3}; \end{cases}$$

$$T = \Sigma p_{x,\lambda,\mu} B_{x,\lambda,\mu};$$

woraus mit Rücksicht auf No. 15. folgt, dafs die Determinante Φ von der Form

$$50. \quad \Phi = Df + \Delta.\varphi$$

ist, wo D und Δ zu bestimmende Constanten bedeuten. Bezeichnet man mit $\Phi(p)$ und $\Phi\left(\frac{1}{\varrho}q\right)$ die Ausdrücke, in welche Φ übergeht, wenn man $p_{x,\lambda,\mu}$ oder $\frac{1}{\varrho}q_{x,\lambda,\mu}$ in der Entwicklung von Φ für $x_x x_\lambda x_\mu$ setzt, so hat man

$$51. \quad RD = \Phi\left(\frac{1}{\varrho}.q\right); \quad R\Delta = \Phi(p);$$

wobei zu bemerken ist, da D verschwindet, wenn δ verschwindet, dafs D den Factor δ haben, oder, da sowohl $\Phi(p)$ als auch $\Phi\left(\frac{1}{\varrho}.q\right)$ ganze homogene Functionen 3ten Grades in Rücksicht auf d und δ sind, dafs in D das mit d^3 multiplicirte Glied fehlen mufs.

Das Vorhergehende läfst sich nun kurz wie folgt ausdrücken:

Lehrsatz 6.

Wenn man eine gegebene homogene Function dreier Variabeln vom dritten Grade und ihre Determinante, die erstere mit d, die andere

mit δ multiplicirt und addirt, so ist die Determinante der Summe der beiden Functionen von derselben Form, nämlich gleich der Summe der gegebenen Function und ihrer Determinante, jede mit einem andern homogenen Factor 3ten Grades in Rücksicht auf d und δ multiplicirt.

Mit Hülfe dieses Lehrsatzes läfst sich leicht folgende Aufgabe lösen:

Aufgabe 1.

Es ist eine homogene Function dritten Grades von drei Variabeln gegeben: man soll eine andere homogene Function 3ten Grades von denselben Variabeln bestimmen, deren Determinante die gegebene Function ist.

Aus dem Lehrsatz (5.) folgt, dafs, wenn f die gegebene Function ist, die gesuchte Function $df+\delta\varphi$ sein wird, wo d und δ aus den Gleichungen

$$D=1 \quad \text{und} \quad \varDelta=0$$

zu bestimmen sind. Die Aufgabe führt also auf eine cubische Gleichung und bietet 9 Auflösungen dar.

19) Wenn man mit f eine beliebige Function der n Variabeln $x_1, x_2, \dots x_n$ bezeichnet, so kann man unter der Annahme folgender linearen Gleichungen:

$$\begin{aligned}
a_1^{(1)}x_1+a_1^{(2)}x_2+\dots+a_1^{(n)}x_n &= y_1,\\
a_2^{(1)}x_1+a_2^{(2)}x_2+\dots+a_2^{(n)}x_n &= y_2,\\
\dots\dots\dots\dots\dots&\\
a_n^{(1)}x_1+a_n^{(2)}x_2+\dots+a_n^{(n)}x_n &= y_n,
\end{aligned}$$

sowohl f als $\frac{\partial f}{\partial x_\varkappa}$ als Functionen der Variabeln $y_1, y_2, \dots y_n$ betrachten. Die Determinanten der Function f seien φ oder φ', je nachdem man $x_1, x_2, \dots x_n$ oder $y_1, y_2, \dots y_n$ als die Variabeln betrachtet. Bezeichnet man nun die aus den Coëfficienten der Variabeln $x_1, x_2, \dots x_n$ in den angegebenen linearen Gleichungen gebildete Determinante mit r, so ist

$$52. \qquad \varphi=r^2\varphi'.$$

Denn wenn n^2 Gröfsen $u_\varkappa^\lambda$ mit n^2 Gröfsen $a_\varkappa^\lambda$ und n^2 Gröfsen $w_\varkappa^\lambda$, wo $\varkappa$, λ die Zahlen 1, 2, ... n bedeuten, in der Verbindung

$$u_\varkappa^\lambda=a_1^\lambda w_1^\varkappa+a_2^\lambda w_2^\varkappa+\dots+a_n^\lambda w_n^\varkappa$$

stehen, so ist bekanntlich die aus den Gröfsen $u_\varkappa^\lambda$ gebildete Determinante $\Sigma\pm u_1^{(1)}u_2^{(2)}\dots u_n^{(n)}$ gleich dem Product zweier Determinanten, von denen die eine r aus den Gröfsen $a_\varkappa^\lambda$, die andere $\Sigma\pm w_1^{(1)}w_2^{(2)}\dots w_n^{(n)}$ aus den Gröfsen $w_\varkappa^\lambda$ zusammengesetzt ist. Diese Relation findet man in der Abhandlung des Herrn Professor *Jacobi*, „De formatione et proprietatibus determinantium"

Bd. 22. dieses Journals S. 310 bewiesen. Ist ferner

$$w_\varkappa^\lambda = a_1^\lambda v_1^\varkappa + a_2^\lambda v_2^\varkappa + \dots + a_n^\lambda v_n^\varkappa,$$

so läfst sich wiederum die Determinante $\Sigma \pm w_1^{(1)} w_2^{(2)} \dots w_n^{(n)}$ als das Product von r und der aus den Gröfsen $v_\varkappa$ gebildeten Determinante $\Sigma \pm v_1^{(1)} v_2^{(2)} \dots v_n^{(n)}$ darstellen. Mithin ist

$$\Sigma \pm u_1^{(1)} u_2^{(2)} \dots u_n^{(n)} = r^2 \Sigma \pm v_1^{(1)} v_2^{(2)} \dots v_n^{(n)}.$$

Die dieser vorhergehenden beiden Gleichungen finden aber Statt, wenn man die Variabeln $x_1, x_2, \dots x_n$ als Functionen der Variabeln $y_1, y_2, \dots y_n$ betrachtet, wie sie durch die obigen n linearen Gleichungen gegeben sind, und setzt:

$$u_\varkappa^\lambda = \frac{\partial^2 f}{\partial x_\varkappa \partial x_\lambda}; \quad w_\lambda^\varkappa = \frac{\partial\left(\frac{\partial f}{\partial x_\varkappa}\right)}{\partial y_\lambda}; \quad v_\varkappa^\lambda = \frac{\partial^2 f}{\partial y_\varkappa \partial y_\lambda}.$$

Diese Werthe von $u_\varkappa^\lambda$ und $v_\varkappa^\lambda$ in die letzte Gleichung gesetzt, welche aus den beiden vorhergehenden folgt, lassen dieselbe in (52.) übergehen. Dieser Gleichung wird man sich bei der Lösung der folgenden Aufgabe mit Vortheil bedienen.

20) Aufgabe 2.

Eine beliebige gegebene homogene Function $f = \Sigma a_{\varkappa,\lambda,\mu} x_\varkappa x_\lambda x_\mu$ *dritten Grades von den Variabeln* x_1, x_2, x_3 *durch Substitutionen von der Form*

$$53. \quad \begin{cases} x_1 = x_1^{(1)} y_1 + x_1^{(2)} y_2 + x_1^{(3)} y_3, \\ x_2 = x_2^{(1)} y_1 + x_2^{(2)} y_2 + x_2^{(3)} y_3, \\ x_3 = x_3^{(1)} y_1 + x_3^{(2)} y_2 + x_3^{(3)} y_3 \end{cases}$$

in eine andere zu transformiren von der Form:

$$54. \quad f = y_1^3 + y_2^3 + y_3^3 + 6\pi y_1 y_2 y_3.$$

Diese Aufgabe verlangt die Bestimmung von 10 Gröfsen: der 9 Coëfcienten der Substitutionen und der Gröfse π. Die 10 Gleichungen, aus welchen die genannten Unbekannten zu bestimmen sind, erhält man, wenn man die Function f der Variabeln x_1, x_2, x_3 in der Gleichung (54.) vermittels der Substitutionen (53.) als eine Function der Variabeln y_1, y_2, y_3 darstellt, nach Potenzen und Producten dieser Variabeln entwickelt und die Coëfficienten gleicher Potenzen und Producte auf beiden Seiten der entwickelten Gleichung einander gleich setzt. Dadurch bekommt man aber Gleichungen von sehr complicirter Art. Dasselbe gilt von den Gleichungen, die sich ergeben, wenn man die Substitutionen (53.) nach y_1, y_2, y_3 auflöset, die Werthe von y_1, y_2, y_3 in den Theil rechts der Gleichung (53.) setzt und die Coëfficien-

ten gleicher Potenzen und Producte der Variabeln y_1, y_2, y_3 auf beiden Seiten der entwickelten Gleichung einander gleich setzt.

Eine dritte Art die Aufgabe zu behandeln ist folgende. Man bilde die Determinante φ' des Theils rechts der Gleichung (54.)

$$55. \quad \varphi' = -6^3\pi^2(y_1^3+y_2^3+y_3^3)+6^3(1+2\pi^3)y_1y_2y_3,$$

bezeichne mit φ, wie vorhin, die Determinante von f, und mit r diejenige aus den Coëfficienten der nach y_1, y_2, y_3 aufgelöseten Gleichungen (53.). Alsdann gilt für den vorliegenden Fall die Gleichung (52.):

$$\varphi = r^2\varphi'.$$

Multiplicirt man die Gleichung (54.) mit $6^3\pi^2r^2$ und addirt sie zu dieser Gleichung, so erhält man

$$6^3.\pi^2.r^2.f+\varphi = 6^3r^2(1+8\pi^3)y_1y_2y_3,$$

welche Gleichung, wenn man der Kürze wegen

$$56. \quad d = \frac{\pi^2}{1+8\pi^3}; \quad \delta = \frac{1}{6^3r^2(1+8\pi^3)}$$

setzt, in

$$57. \quad d.f+\delta.\varphi = y_1y_2y_3$$

übergeht. Diese Gleichung läfst sich in Worten wie folgt ausdrücken:

Lehrsatz 7.

Eine gegebene homogene Function dritten Grades von drei Variabeln, so wie ihre Determinante, lassen sich mit solchen constanten Factoren multipliciren, dafs die Summe in drei lineäre Factoren zerlegbar ist.

Ferner ist zu bemerken, dafs die vorliegende Aufgabe mit folgender übereinkommt: *Eine gegebene homogene Function dritten Grades von drei Variabeln, und ihre Determinante, mit solchen Factoren zu multipliciren, dafs ihre Summe in lineäre Factoren zerlegbar sei.*

Um diese constanten Factoren zu finden, bemerke man, dafs sowohl der Theil links der Gleichung (57.), als seine nach x_1, x_2, x_3 genommenen partiellen Differentialquotienten für die Werthe $x_1^{(\varkappa)}$, $x_2^{(\varkappa)}$, $x_3^{(\varkappa)}$ der Variabeln x_1, x_2, x_3, wo $\varkappa$ eine der Zahlen 1, 2, 3 bedeutet, verschwinden, weil der Theil rechts der Gleichung und seine nach x_1, x_2, x_3 genommenen partiellen Differentialquotienten für die nach (53.) entsprechenden Werthe $y_2=0$, $y_3=0$ oder $y_3=0$, $y_1=0$ oder $y_1=0$, $y_2=0$ verschwinden Man hat daher, mit Beibehaltung der frühern Bezeichnungen, für die Werthe $x_1=x_1^{(\varkappa)}$, $x_2=x_2^{(\varkappa)}$, $x_3=x_3^{(\varkappa)}$.

$$58. \quad d.f_1+\delta.\varphi_1=0; \quad d.f_2+\delta.\varphi_2=0; \quad d.f_3+\delta.\varphi_3=0;$$

woraus nach Lehrsatz 3. folgt:

$$59. \quad D.f_1+\varDelta.\varphi_1=0; \quad D.f_2+\varDelta.\varphi_2=0; \quad D.f_3+\varDelta.\varphi_3=0.$$

Eliminirt man endlich f_1 oder f_2 oder f_3, so erhält man zwischen d und δ die Bedingungsgleichung

$$60. \quad D.\delta-\varDelta.d=0.$$

Diese Gleichung ist homogen in Rücksicht auf d und δ und vom 4ten Grade, weil, wie sich in No. 18. zeigte, D und $\varDelta$ homogen und vom dritten Grade sind. Demnach läfst sich der Lehrsatz 7. wie folgt vervollständigen.

Lehrsatz 8.

Eine gegebene homogene Function 3ten Grades von drei Variabeln und ihre Determinante lassen sich auf 4 verschiedene Arten mit solchen constanten Factoren multipliciren, dafs die Summe jedesmal in lineäre Factoren zerlegbar ist.

Wenn man die Elimination der Variabeln x_1, x_2, x_3 aus (58.) und (59.) auf die Weise ausgeführt hätte, dafs man in der Entwicklung derselben nach Potenzen und Producten der Variabeln diese Potenzen und Producte als die Unbekannten eliminirte, so würde man eine homogene Gleichung vom 12ten Grade in Rücksicht auf d und δ erhalten haben; woraus man schliefsen könnte, dafs es nicht 4 sondern 12 Arten der Zerlegung in lineäre Factoren gebe. Von diesen 12 Arten fallen aber immer je drei in eine zusammen, weil die aus der genannten Elimination hervorgehende Endgleichung von der Form $(D.\delta-\varDelta.d)^3=0$ ist; was aus dem Vorhergehenden erhellt.

Dividirt man die Gleichung (60.) durch δ^4, so wird man eine Gleichung 4ten Grades in Rücksicht auf die Unbekannte $\frac{d}{\delta}$ erhalten, deren Wurzeln

$$\left(\frac{d}{\delta}\right)_1, \quad \left(\frac{d}{\delta}\right)_2, \quad \left(\frac{d}{\delta}\right)_3, \quad \left(\frac{d}{\delta}\right)_4$$

sind. Diese 4 Wurzeln sind zu bestimmen, wenn man die vorgelegte Aufgabe vollständig lösen will. Ist es geschehn und läfst man d und δ irgend zwei Gröfsen bedeuten, deren Quotient $\frac{d}{\delta}$ einer der gefundenen Wurzeln gleich ist, so bleiben noch die Gleichungen (58.) aufzulösen, aus denen man die Verhältnisse der Unbekannten $x_1:x_2:x_3$ festzustellen hat. Es ist aber oben angedeutet worden, dafs diese Gleichungen erfüllt werden, wenn man für x_1, x_2, x_3 entweder $x_1^{(1)}$, $x_2^{(1)}$, $x_3^{(1)}$ oder $x_1^{(2)}$, $x_2^{(2)}$, $x_3^{(2)}$ oder $x_1^{(3)}$, $x_2^{(3)}$, $x_3^{(3)}$

setzt. Man wird daher drei verschiedene Systeme von Verhältnissen der Unbekannten zu einander aus den Gleichungen (58.) ziehen können, welche jenen Gleichungen genügen. Löset man aber zwei von den Gleichungen (58.) auf, so ergeben sich, da sie vom zweiten Grade sind, 4 solcher Systeme, von denen eines, welches der Gleichung (58.) nicht genügt, auszusondern ist. Wie die Unbequemlichkeit der Aussonderung des 4ten, überflüssigen Systems durch einen eleganten Calcul vermieden werden könne, soll in dem nächstfolgenden Paragraph auseinandergesetzt werden. Hat man nun auf irgend eine Weise die drei verschiedenen Systeme von Verhältnissen der Unbekannten gefunden, welche sämmtlichen Gleichungen (58.) genügen; so wird jedes derselben einem Systeme der Verhältnisse der unbekannten Coëfficienten $x_1^{(x)} : x_2^{(x)} : x_3^{(x)}$ gleich sein. Damit die Unbekannten aber den gesuchten Coëfficienten der Substitutionen selbst gleich werden, hat man sie so zu bestimmen, dafs sie noch der Gleichung

$$f = 1$$

genügen. Nachdem auf diese Weise die gesuchten Coëfficienten der Substitutionen bestimmt worden sind, bleibt noch übrig, den Werth der Gröfse π in der Gleichung (54.) anzugeben. Dieser ergiebt sich aus der genannten Gleichung, wenn man den Theil links derselben durch die gefundenen Substitutionen als eine Function der Variabeln y_1, y_2, y_3 darstellt, den Coëfficienten von $y_1 y_2 y_3$ der Entwicklung heraushebt und ihn durch die Zahl 6 dividirt.

Die vorgelegte Aufgabe läfst vier wesentlich von einander verschiedene Auflösungen zu, da man auf die angegebene Art jede der vier Wurzeln der Gleichung (60.) verwenden kann.

21) Nachdem man die Wurzeln der biquadratischen Gleichung (60.) berechnet und zwei Gröfsen d und δ bestimmt hat, deren Quotient $\frac{d}{\delta}$ gleich einer jener Wurzeln ist, so bleibt noch übrig, die drei verschiedenen Verhältnisse der Unbekannten $x_1 : x_2 : x_3$ zu bestimmen, welche sämmtlichen Gleichungen (58.) genügen. Dieses kann auf folgende Weise geschehen. Man setze die Werthe von φ_1, φ_2, φ_3 aus (58.) in die Gleichungen (33.*). Diese Gleichungen lassen sich, wenn man α, β, γ für Rx_1, Rx_2, Rx_3 setzt, wie folgt darstellen:

$$61.\quad\begin{cases}
\alpha x_1 = \left(\frac{1}{\varrho}q_{1,1,1}-\frac{d}{\delta}p_{1,1,1}\right)f_1+\left(\frac{1}{\varrho}q_{1,1,2}-\frac{d}{\delta}p_{1,1,2}\right)f_2+\left(\frac{1}{\varrho}q_{1,1,3}-\frac{d}{\delta}p_{1,1,3}\right)f_3,\\
\alpha x_2 = \left(\frac{1}{\varrho}q_{1,2,1}-\frac{d}{\delta}p_{1,2,1}\right)f_1+\left(\frac{1}{\varrho}q_{1,2,2}-\frac{d}{\delta}p_{1,2,2}\right)f_2+\left(\frac{1}{\varrho}q_{1,2,3}-\frac{d}{\delta}p_{1,2,3}\right)f_3,\\
\alpha x_3 = \left(\frac{1}{\varrho}q_{1,3,1}-\frac{d}{\delta}p_{1,3,1}\right)f_1+\left(\frac{1}{\varrho}q_{1,3,2}-\frac{d}{\delta}p_{1,3,2}\right)f_2+\left(\frac{1}{\varrho}q_{1,3,3}-\frac{d}{\delta}p_{1,3,3}\right)f_3,\\
\beta x_1 = \left(\frac{1}{\varrho}q_{2,1,1}-\frac{d}{\delta}p_{2,1,1}\right)f_1+\left(\frac{1}{\varrho}q_{2,1,2}-\frac{d}{\delta}p_{2,1,2}\right)f_2+\left(\frac{1}{\varrho}q_{2,1,3}-\frac{d}{\delta}p_{2,1,3}\right)f_3,\\
\beta x_2 = \left(\frac{1}{\varrho}q_{2,2,1}-\frac{d}{\delta}p_{2,2,1}\right)f_1+\left(\frac{1}{\varrho}q_{2,2,2}-\frac{d}{\delta}p_{2,2,2}\right)f_2+\left(\frac{1}{\varrho}q_{2,2,3}-\frac{d}{\delta}p_{2,2,3}\right)f_3,\\
\beta x_3 = \left(\frac{1}{\varrho}q_{2,3,1}-\frac{d}{\delta}p_{2,3,1}\right)f_1+\left(\frac{1}{\varrho}q_{2,3,2}-\frac{d}{\delta}p_{2,3,2}\right)f_2+\left(\frac{1}{\varrho}q_{2,3,3}-\frac{d}{\delta}p_{2,3,3}\right)f_3,\\
\gamma x_1 = \left(\frac{1}{\varrho}q_{3,1,1}-\frac{d}{\delta}p_{3,1,1}\right)f_1+\left(\frac{1}{\varrho}q_{3,1,2}-\frac{d}{\delta}p_{3,1,2}\right)f_2+\left(\frac{1}{\varrho}q_{3,1,3}-\frac{d}{\delta}p_{3,1,3}\right)f_3,\\
\gamma x_2 = \left(\frac{1}{\varrho}q_{3,2,1}-\frac{d}{\delta}p_{3,2,1}\right)f_1+\left(\frac{1}{\varrho}q_{3,2,2}-\frac{d}{\delta}p_{3,2,2}\right)f_2+\left(\frac{1}{\varrho}q_{3,2,3}-\frac{d}{\delta}p_{3,2,3}\right)f_3,\\
\gamma x_3 = \left(\frac{1}{\varrho}q_{3,3,1}-\frac{d}{\delta}p_{3,3,1}\right)f_1+\left(\frac{1}{\varrho}q_{3,3,2}-\frac{d}{\delta}p_{3,3,2}\right)f_2+\left(\frac{1}{\varrho}q_{3,3,3}-\frac{d}{\delta}p_{3,3,3}\right)f_3.
\end{cases}$$

Durch Auflösung des ersten, zweiten und letzten Systems von 3 Gleichungen nach f_1, f_2, f_3 erhält man:

$$62.\quad\begin{cases}
f_1 = \alpha(a_{1,1}x_1+a_{1,2}x_2+a_{1,3}x_3),\\
f_2 = \alpha(a_{2,1}x_1+a_{2,2}x_2+a_{2,3}x_3),\\
f_3 = \alpha(a_{3,1}x_1+a_{3,2}x_2+a_{3,3}x_3),\\
f_1 = \beta(b_{1,1}x_1+b_{1,2}x_2+b_{1,3}x_3),\\
f_2 = \beta(b_{2,1}x_1+b_{2,2}x_2+b_{2,3}x_3),\\
f_3 = \beta(b_{3,1}x_1+b_{3,2}x_2+b_{3,3}x_3),\\
f_1 = \gamma(c_{1,1}x_1+c_{1,2}x_2+c_{1,3}x_3),\\
f_2 = \gamma(c_{2,1}x_1+c_{2,2}x_2+c_{2,3}x_3),\\
f_3 = \gamma(c_{3,1}x_1+c_{3,2}x_2+c_{3,3}x_3);
\end{cases}$$

wobei zu bemerken ist, dafs $a_{\varkappa,\lambda}=a_{\lambda,\varkappa}$ und eben so $b_{\varkappa,\lambda}=b_{\lambda,\varkappa}$ und $c_{\varkappa,\lambda}=c_{\lambda,\varkappa}$. Zieht man nun das zweite System der Gleichungen (62.) von dem ersten ab, so erhält man:

$$63.\quad\begin{cases}
\left(\frac{\alpha}{\beta}a_{1,1}-b_{1,1}\right)x_1+\left(\frac{\alpha}{\beta}a_{1,2}-b_{1,2}\right)x_2+\left(\frac{\alpha}{\beta}a_{1,3}-b_{1,3}\right)x_3 = 0,\\
\left(\frac{\alpha}{\beta}a_{2,1}-b_{2,1}\right)x_1+\left(\frac{\alpha}{\beta}a_{2,2}-b_{2,2}\right)x_2+\left(\frac{\alpha}{\beta}a_{2,3}-b_{2,3}\right)x_3 = 0,\\
\left(\frac{\alpha}{\beta}a_{3,1}-b_{3,1}\right)x_1+\left(\frac{\alpha}{\beta}a_{3,2}-b_{3,2}\right)x_2+\left(\frac{\alpha}{\beta}a_{3,3}-b_{3,3}\right)x_3 = 0;
\end{cases}$$

woraus sich durch Elimination der Unbekannten x_1, x_2, x_3 eine Gleichung

dritten Grades in Rücksicht auf $\frac{\alpha}{\beta}$ wie

$$64.\quad W = 0$$

ergiebt. Die Wurzeln dieser Gleichung seien:

$$\left(\frac{\alpha}{\beta}\right)^{(1)},\quad \left(\frac{\alpha}{\beta}\right)^{(2)},\quad \left(\frac{\alpha}{\beta}\right)^{(3)}.$$

Setzt man dieselben nach einander in (63.) und bestimmt für jede die entsprechenden Verhältnisse der Unbekannten, so werden solche gleich den Verhältnissen der Coëfficienten $x_1^{(\varkappa)}$, $x_2^{(\varkappa)}$, $x_3^{(\varkappa)}$ der Substitutionen sein, wenn man sie aus den angegebenen Gleichungen (63.) und der Gleichung $f = 1$ bestimmt.

Es ist im Vorhergehenden angedeutet worden, dafs die vorgelegte Aufgabe 4 wesentlich von einander verschiedene Lösungen zuläfst. Man erhält zwar aus den gefundenen Auflösungen andere, wenn man für die Variabeln y_1, y_2, y_3 dieselben Variabeln mit den dritten Wurzeln der Einheit multiplicirt setzt. Diese werden aber nicht als wesentlich verschieden zu betrachten sein. Jede der 4 verschiedenen Auflösungen verlangt die Kenntnifs einer Wurzel der biquadratischen Gleichung (60.) und der vollständigen Auflösung der dieser Wurzel entsprechenden cubischen Gleichung (64.). Die vollständige Lösung der Aufgabe verlangt also die Auflösung einer biquadratischen Gleichung und 4 von den Wurzeln derselben abhängigen cubischen Gleichungen. In der folgenden Nummer soll aber dargethan werden, wie aus der einen Auflösung der Aufgabe die übrigen abgleitet werden können, ohne die Auflösung einer höheren Gleichung. Die Ausziehung der dritten Wurzel aus der Einheit wird hiebei nicht für eine Auflösung einer cubischen Gleichung gerechnet. Dieses vorausgesetzt, so erhellet, dafs die vollständige Lösung der Aufgabe in der That nur die Kenntnifs einer Wurzel der biquadratischen Gleichung (60.) und die vollständige Auflösung der von dieser Wurzel abhängigen cubischen Gleichung (64.) verlangt.

22) **Aufgabe 3.**

Die gegebene Function

$$f = y_1^3 + y_2^3 + y_3^3 + 6\pi y_1 y_2 y_3$$

durch Substitutionen von der Form

$$\begin{aligned} y_1 &= y_1^{(1)} z_1 + y_1^{(2)} z_2 + y_1^{(3)} z_3, \\ y_2 &= y_2^{(1)} z_1 + y_2^{(2)} z_2 + y_2^{(3)} z_3, \\ y_3 &= y_3^{(1)} z_1 + y_3^{(2)} z_2 + y_3^{(3)} z_3 \end{aligned}$$

in andere von derselben Form

$$66.\quad f = z_1^3 + z_2^3 + z_3^3 + 6\Pi . z_1 z_2 z_3$$

zu transformiren.

Wenn man diese Aufgabe auf dem in No. 20. angegebenen Wege zu lösen unternimmt, so wird man finden, dafs die Bestimmung der Verhältnisse der Coëfficienten $y_1^{(\nu)}$, $y_2^{(\nu)}$, $y_3^{(\nu)}$ auf die Lösung der Gleichungen

$$58. \quad y_1^2 - \lambda y_2 y_3 = 0; \quad y_2^2 - \lambda y_3 y_1 = 0; \quad y_3^2 - \lambda y_1 y_2 = 0$$

führt, welche in der vorhergehenden Aufgabe den Gleichungen (58.) entsprechen. Durch Elimination der Variabeln y_1, y_2, y_3 erhält man die der Gleichung (60.) entsprechende Gleichung $\quad$ 60.* $\quad \lambda^3 = 1$.

Bezeichnet man nun durch k' und k'' die beiden imaginären dritten Wurzeln der Einheit, so giebt (58.*):

für $\lambda = 1$,	für $\lambda = k'$,	für $\lambda = k''$,
$y_1 : y_2 : y_3 = 1:1:1$,	$y_1 : y_2 : y_3 = 1:k':k'$,	$y_1 : y_2 : y_3 = 1:k'':k''$,
$y_1 : y_2 : y_3 = 1:k':k''$,	$y_1 : y_2 : y_3 = 1:1:k''$,	$y_1 : y_2 : y_3 = 1:1:k'$,
$y_1 : y_2 : y_3 = 1:k'':k'$,	$y_1 : y_2 : y_3 = 1:k'':1$,	$y_1 : y_2 : y_3 = 1:k':1$;

woraus folgende drei Substitutionen hervorgehen, durch welche die gegebene Function f der Variabeln y_1, y_2, y_3 in andere von derselben Form transformirt wird:

Erste Substitution.

$$67. \begin{cases} 3(1+2\pi)y_1 = z_1 + z_2 + z_3 & \text{oder} \quad z_1 = (1+2\pi)\{y_1 + y_2 + y_3\}, \\ 3(1+2\pi)y_2 = z_1 + k' z_2 + k'' z_3 & - \quad z_2 = (1+2\pi)\{y_1 + k'' y_2 + k' y_3\}, \\ 3(1+2\pi)y_3 = z_1 + k'' z_2 + k' z_3 & - \quad z_3 = (1+2\pi)\{y_1 + k' y_2 + k'' y_3\}. \end{cases}$$

Zweite Substitution.

$$68. \begin{cases} 3(1+2k''\pi)y_1 = z_1 + z_2 + z_3 & \text{oder} \quad k' z_1 = (1+2k''\pi)\{k' y_1 + y_2 + y_3\}, \\ 3(1+2k''\pi)y_2 = k' z_1 + z_2 + k'' z_3 & - \quad z_2 = (1+2k''\pi)\{y_1 + y_2 + k' y_3\}, \\ 3(1+2k''\pi)y_3 = k' z_1 + k'' z_2 + z_3 & - \quad z_3 = (1+2k''\pi)\{y_1 + k' y_2 + y_3\}. \end{cases}$$

Dritte Substitution.

$$69. \begin{cases} 3(1+2k'\pi)y_1 = z_1 + z_2 + z_3 & \text{oder} \quad k'' z_1 = (1+2k'\pi)\{k'' y_1 + y_2 + y_3\}, \\ 3(1+2k'\pi)y_2 = k'' z_1 + z_2 + k' z_3 & - \quad z_2 = (1+2k'\pi)\{y_1 + y_2 + k'' y_3\}, \\ 3(1+2k'\pi)y_3 = k'' z_1 + k' z_2 + z_3 & - \quad z_3 = (1+2k'\pi)\{y_1 + k'' y_2 + y_3\}. \end{cases}$$

Die verschiedenen Substitutionen, durch welche eine gegebene Function $f = \Sigma a_{\varkappa,\lambda,\mu} x_\varkappa x_\lambda x_\mu$ der Variabeln x_1, x_2, x_3 in andere von der Form

$$z_1^3 + z_2^3 + z_3^3 + 6\Pi z_1 z_2 z_3$$

transformirt wird, erhält man nun, wenn man in den Substitutionen (53.), deren Coëfficienten in No. 20. und 21. bestimmt worden sind, für y_1, y_2, y_3 entweder z_1, z_2, z_3 oder die Werthe von y_1, y_2, y_3 aus den vorhergehenden drei Substitutionen setzt. Aus diesen Substitutionen ergeben sich endlich noch andere, wenn man die Variabeln z_1, z_2, z_3 einzeln mit den dritten Wurzeln der Einheit multiplicirt und diese Producte statt der Variabeln z_1, z_2, z_3 setzt. (Die Fortsetzung im nächsten Heft.)

Königsberg, den 16. Januar 1844.

Fac-simile einer ...

Clarissimo atque

Dn. Dn.
Joan. Wallis
Londinum.

Quod adeo humanissimis
longographicis tam praeclar(e)
singulari ornari elogio
erga me propensissimum
cognosco, sed etiam grat(um)
te nepimonere hoc nomine
tuam mihi in promovendo
computandi profectum long(e)
in eandem sententiam, a
viam sollicitus fui de is
quia occupationes meae,
variae, ut vix potuerim
operosissimus labor, a me
versi, praecepto, a te mih(i)
operam in rei literariae
tempore ne non tergiversa(r)

11.

Über die Wendepuncte der Curven dritter Ordnung.

(Von Herrn Dr. *Otto Hesse*, Privatdocenten an der Universität zu Königsberg.)

(Fortsetzung der Abhandlung No. 10. im vorigen Heft: „Über die Elimination der Variabeln aus algebraischen Gleichungen zweiten Grades.")

---

23) Wenn man mit x_1, x_2 die rechtwinkligen Coordinaten eines Punctes p in der Ebene bezeichnet, der auf einer durch ihre Gleichung $u=0$ gegebenen Curve beliebig aber fest angenommen ist: ferner mit X_1, X_2 die Coordinaten eines variabeln Punctes der in dem ersten Puncte errichteten Normale der Curve, so verhalten sich die Differenzen x_1-X_1, x_2-X_2 wie die Cosinusse der Winkel, welche die Normale mit den Coordinaten-Axen bildet, oder wie die partiellen Differentialquotienten u_1, u_2 der Function u der Variabeln x_1, x_2, nach diesen Variabeln genommen. Bezeichnet man ferner durch λ einen unbestimmten variabeln Factor, so hat man

$$65. \quad (x_1-X_1)\lambda = u_1, \quad (x_2-X_2)\lambda = u_2,$$

woraus durch die Elimination von λ die Gleichung der Normale selbst hervorgeht. Diese Elimination kann jedoch unterbleiben, da es vortheilhafter ist, die Gleichungen der Normale unter der Form (65.) zu betrachten.

Bezeichnet man mit x_1+dx_1, x_2+dx_2 die Coordinaten eines dem Puncte p unendlich nahe gelegenen Punctes der Curve $u=0$, und mit μ einen unbestimmten variablen Factor, so erhält man für die den vorhergehenden entsprechenden Gleichungen der in diesem Puncte errichteten Normale:

$$(x_1+dx_1-X_1)\mu = u_1+du_1, \quad (x_2+dx_2-X_2)\mu = u_2+du_2.$$

Für den Krümmungsmittelpunct der Curve, in welchem sich, wie bekannt, die beiden Normalen schneiden, gelten die angegebenen 4 Gleichungen. Läfst man daher X_1, X_2 die Coordinaten des Krümmungsmittelpunctes bedeuten, so kann man dieselben mit Hülfe der angegebenen Gleichungen und der folgenden durch die Coordinaten des Punctes p wie folgt ausdrücken:

$$u_1dx_1+u_2dx_2 = 0.$$

Die Länge ϱ des Krümmungshalbmessers ergiebt sich aber aus der Formel $\varrho=\sqrt{((x_1-X_1)^2+(x_2-X_2)^2)}$ oder

$$66. \quad \varrho = \frac{1}{\lambda}\sqrt{(u_1^2+u_2^2)}.$$

Es bleibt nun noch übrig, den Werth von λ anzugeben. Denn hat man diesen gefunden, so giebt die Gleichung (66.) den Werth des Krümmungsradius, und (65.) giebt die Relationen, welche zwischen den Coordinaten des Punctes p und den Coordinaten X_1, X_2 des Krümmungsradius Statt finden. Zu diesem Zwecke ziehe man die Gleichungen (65.) von den darauf folgenden beiden ab. Dieses giebt

$$(x_1+dx_1-X_1)(\mu-\lambda) = du_1-\lambda dx_1, \quad (x_2+dx_2-X_2)(\mu-\lambda) = du_2-\lambda dx_2$$

und, wenn man die Werthe von x_1-X_1 und x_2-X_2 aus (65.) setzt,

$$(u_1+\lambda dx_1)\frac{\mu-\lambda}{\lambda} = du_1-\lambda dx_1, \quad (u_2+\lambda dx_2)\frac{\mu-\lambda}{\lambda} = du_2-\lambda dx_2.$$

Vernachlässigt man die unendlich kleinen Gröfsen λdx_1, λdx_2 gegen die endlichen u_1, u_2, so hat man

$$u_1\frac{\mu-\lambda}{\lambda} = du_1-\lambda dx_1, \quad u_2\frac{\mu-\lambda}{\lambda} = du_2-\lambda dx_2.$$

Fügt man hiezu noch die Gleichung $u_1dx_1+u_2dx_2=0$ und bezeichnet die zweiten partiellen Differentialquotienten $\frac{\partial^2 u}{\partial x_\varkappa \partial x_\lambda}$ der Function u der Kürze wegen mit $u_{\varkappa,\lambda}$, so stellen sich diese Gleichungen wie folgt dar:

$$u_1\frac{\mu-\lambda}{\lambda} = (u_{1,1}-\lambda)dx_1+u_{1,2}dx_2, \quad u_2\frac{\mu-\lambda}{\lambda} = u_{2,1}dx_1+(u_{2,2}-\lambda)dx_2,$$
$$u_1dx_1+u_2dx_2 = 0.$$

Wenn man die beiden ersten Gleichungen nach dx_1 und dx_2 auflöset, so erhält man

$$Ndx_1 = (u_{2,2}-\lambda)u_1-u_{1,2}u_2, \quad Ndx_2 = -u_{2,1}u_1+(u_{1,1}-\lambda)u_2,$$
$$N = \frac{\lambda}{\mu-\lambda}\{(u_{1,1}-\lambda)(u_{2,2}-\lambda)-u_{1,2}u_{2,1}\},$$

und wenn man diese Werthe von dx_1 und dx_2 in die letzte Gleichung setzt,

$$u_1^2(u_{2,2}-\lambda)-2u_1u_2u_{1,2}+u_2^2(u_{1,1}-\lambda) = 0.$$

Daraus ergiebt sich für den gesuchten Werth von λ:

$$67. \quad \lambda = \frac{u_1^2u_{2,2}-2u_1u_2u_{1,2}+u_2^2u_{1,1}}{u_1^2+u_2^2}.$$

24. Es seien x_1, x_2, x_3 die rechtwinkligen Coordinaten eines Punctes p einer durch die Gleichung $u=0$ gegebenen Oberfläche, X_1, X_2, X_3 die Coordinaten eines variabeln Punctes der in p errichteten Normale der Oberfläche. Unter dieser Voraussetzung verhalten sich die Differenzen $x_1=X_1$, x_2-X_2, x_3-X_3 wie die Cosinusse der Winkel, welche die Normale mit den Coordinaten-Axen bildet, oder wie die partiellen Differentialquotienten u_1, u_2, u_3 der Function u, nach den Variabeln x_1, x_2, x_3 genommen. Es

sind daher, wenn man mit λ einen unbestimmten variabeln Factor bezeichnet, die Gleichungen der im Puncte p errichteten Normale der Oberfläche folgende:

$$68.\quad (x_1-X_1)\lambda = u_1,\quad (x_2-X_2)\lambda = u_2,\quad (x_3-u_3)\lambda = X_3.$$

Ebenso wird die in einem dem Puncte p auf der Oberfläche unendlich nahe gelegenen Puncte q errichtete Normale, wenn man mit x_1+dx_1, x_2+dx_2, x_3+dx_3 die Coordinaten dieses Punctes und mit μ einen unbestimmten variabeln Factor bezeichnet, durch die Gleichungen bestimmt:

$$\begin{aligned}(x_1+dx_1-X_1)\mu &= u_1+du_1,\\ (x_2+dx_2-X_2)\mu &= u_2+du_2,\\ (x_3+dx_3-X_3)\mu &= u_3+du_3.\end{aligned}$$

Diese beiden Normalen werden sich im Allgemeinen nicht schneiden. Sie schneiden sich aber, wenn der Punct q auf der durch p gehenden Krümmungslinie der Oberfläche angenommen wird, in welchem Falle der Schnittpunct r der Normalen zu dem Krümmungsmittelpunct des durch p und q gelegten Hauptschnittes wird. Läfst man daher X_1, X_2, X_3 die Coordinaten dieses Krümmungsmittelpunctes bedeuten, so ergeben sich die Werthe derselben aus den angegebenen, zu gleicher Zeit Statt findenden beiden Systemen von Gleichungen, und der Krümmungsradius ist $\varrho = \sqrt{((x_1-X_1)^2+(x_2-X_2)^2+(x_3-X_3)^2)}$, oder, mit Rücksicht auf (68.):

$$69\quad \varrho = \frac{1}{\lambda}\sqrt{(u_1^2-u_2^2-u_3^2)}).$$

Um den Werth von λ in dieser Formel zu bestimmen, ziehe man die Gleichungen der Normalen von einander ab. Dieses giebt

$$\begin{aligned}(x_1+dx_1-X_1)(\mu-\lambda) &= du_1-\lambda dx_1,\\ (x_2+dx_2-X_2)(\mu-\lambda) &= du_2-\lambda dx_2,\\ (x_3+dx_3-X_3)(\mu-\lambda) &= du_3-\lambda dx_3.\end{aligned}$$

Diese Gleichungen gehen, wenn man die unendlich kleinen Gröfsen dx_1, dx_2, dx_3 im Verhältnifs zu den endlichen Differenzen x_1-X_1, x_2-X_2, x_3-X_3 vernachlässigt und für die Differenzen die Werthe aus (68.) setzt, in folgende über:

$$u_1\frac{\mu-\lambda}{\lambda} = du_1-\lambda dx_1,\quad u_2\frac{\mu-\lambda}{\lambda} = du_2-\lambda dx_2,\quad u_3\frac{\mu-\lambda}{\lambda} = du_3-\lambda dx_3.$$

Fügt man noch die Differentialgleichung der Oberfläche hinzu und bezeichnet die Differentialquotienten $\frac{\partial^2 u}{\partial x_x \partial x_\lambda}$ der Kürze wegen mit $u_{x,\lambda}$, so lassen sich die Gleichungen wie folgt darstellen:

$$u_1\frac{\mu-\lambda}{\lambda} = (u_{1,1}-\lambda)dx_1+u_{1,2}dx_2+u_{1,3}dx_3,$$
$$u_2\frac{\mu-\lambda}{\lambda} = u_{2,1}dx_1+(u_{2,2}-\lambda)dx_2+u_{2,3}dx_3,$$
$$u_3\frac{\mu-\lambda}{\lambda} = u_{3,1}dx_1+u_{3,2}dx_2+(u_{3,3}-\lambda)dx_3,$$
$$u_1dx_1+u_2dx_2+u_3dx_3 = 0.$$

Aus den drei ersten Gleichungen ergeben sich die Werthe von dx_1, dx_2, dx_3 durch Auflösung. Setzt man dieselben in die letzte Gleichung, so wird man finden:

$$0=\begin{cases} u_1^2\{(u_{2,2}-\lambda)(u_{3,3}-\lambda)-u_{2,3}^2\}+u_2^2\{(u_{3,3}-\lambda)(u_{1,1}-\lambda)-u_{3,1}^2\}+u_3^2\{(u_{1,1}-\lambda)(u_{2,2}-\lambda)-u_{1,2}^2\} \\ +2u_2u_3\{u_{2,1}u_{3,1}-(u_{1,1}-\lambda)u_{2,3}\}+2u_3u_1\{u_{3,2}u_{1,2}-(u_{2,2}-\lambda)u_{3,1}\} \\ \qquad +2u_1u_2\{u_{1,3}u_{2,3}-(u_{3,3}-\lambda)u_{1,2}\}. \end{cases}$$

Bezeichnet man endlich mit λ_1 und λ_2 die beiden Wurzeln der vorliegenden quadratischen Gleichung, so erhält man:

$$70.\quad \lambda_1+\lambda_2 = \frac{u_1^2(u_{2,2}+u_{3,3})+u_2^2(u_{3,3}+u_{1,1})+u_3^2(u_{1,1}+u_{2,2})-2u_2u_3u_{2,3}-2u_3u_1u_{3,1}-2u_1u_2u_{1,2}}{u_1^2+u_2^2+u_3^2};$$

$$71.\quad \lambda_1\lambda_2 = \frac{u_1^2V_{1,1}+u_2^2V_{2,2}+u_3^2V_{3,3}+2u_2u_3V_{2,3}+2u_3u_1V_{3,1}+2u_1u_2V_{1,2}}{u_1^2+u_2^2+u_3^2},$$

wo die Gröfsen $V_{\varkappa,\lambda}$ die Bedeutung

$$V_{1,1} = u_{2,2}u_{3,3}-u_{2,3}^2,\qquad V_{2,3} = u_{2,1}u_{3,1}-u_{1,1}u_{2,3},$$
$$V_{2,2} = u_{3,3}u_{1,1}-u_{3,1}^2,\qquad V_{3,1} = u_{3,2}u_{1,2}-u_{2,2}u_{3,1},$$
$$V_{3,3} = u_{1,1}u_{2,2}-u_{1,2}^2,\qquad V_{1,2} = u_{1,3}u_{2,3}-u_{3,3}u_{1,2}$$

haben. Wenn man diese Wurzeln nach einander in (69.) statt λ setzt, so erhält man die Krümmungsradien der Hauptschnitte im Puncte p der Oberfläche. Setzt man sie in (68.), so bestimmen jene Gleichungen die Coordinaten X_1, X_2, X_3 der Krümmungsmittelpuncte der Hauptschnitte.

Die Zähler der Ausdrücke (67.) und (71.) kann man auf eine elegante Art transformiren, wenn u eine ganze algebraische Function vom Grade n ist. Diese Transformation soll in Folgendem auseinandergesetzt werden.

25) Durch Auflösung eines lineären Systems von Gleichungen mit m Unbekannten x_1, x_2, ... x_m von der Form

$$72.\quad \begin{cases} U_1 = x_1u_{1,1}+x_2u_{1,2}+\dots+x_mu_{1,m}, \\ U_2 = x_1u_{2,1}+x_2u_{2,2}+\dots+x_mu_{2,m}, \\ \dots\dots\dots\dots\dots\dots \\ U_m = x_1u_{m,1}+x_2u_{m,2}+\dots+x_mu_{m,m} \end{cases}$$

erhält man Gleichungen von der Form:

$$73.\quad \begin{cases} \Delta.x_1 = U_1 U_{1,1} + U_2 U_{2,1} + \dots + U_m U_{m,1}, \\ \Delta.x_2 = U_1 U_{1,2} + U_2 U_{2,2} + \dots + U_m U_{m,2}, \\ \dots\dots\dots\dots\dots\dots \\ \Delta.x_m = U_1 U_{1,m} + U_2 U_{2,m} + \dots + U_m U_{m,m}, \end{cases}$$

wo Δ die aus den Coëfficienten der Gleichungen (72.) zusammengesetzte Determinante, also eine ganze Function vom Grade m und die Gröfsen $U_{x,\lambda}$ ganze Functionen vom Grade $m-1$ in Rücksicht auf die genannten Coëfficienten bedeuten.

Ein zweites gegebenes System lineärer Gleichungen mit den $m-1$ Unbekannten $x_1, x_2, \dots x_{m-1}$

$$74.\quad \begin{cases} V_1 = x_1 u_{1,1} + x_2 u_{1,2} + \dots + x_{m-1} u_{1,m-1}, \\ V_2 = x_1 u_{2,1} + x_2 u_{2,2} + \dots + x_{m-1} u_{2,m-1}, \\ \dots\dots\dots\dots\dots\dots \\ V_{m-1} = x_1 u_{m-1,1} + x_2 u_{m-1,2} + \dots + x_{m-1} u_{m-1,m-1} \end{cases}$$

gebe, nach den Unbekannten aufgelöset,

$$75.\quad \begin{cases} \delta.x_1 = V_1 V_{1,1} + V_2 V_{2,1} + \dots + V_{m-1} V_{m-1,1}, \\ \delta.x_2 = V_1 V_{1,2} + V_2 V_{2,2} + \dots + V_{m-1} V_{m-1,2}, \\ \dots\dots\dots\dots\dots\dots \\ \delta.x_{m-1} = V_1 V_{1,m-1} + V_2 V_{2,m-1} + \dots + V_{m-1} V_{m-1,m-1}. \end{cases}$$

In diesen Gleichungen bedeutet δ die aus den Coëfficienten der Gleichungen (74.) zusammengesetzte Determinante, welche mit der Determinante Δ in der Verbindung

$$76.\quad \frac{\partial \Delta}{d u_{m,m}} = \delta = X_{m,m}$$

steht. Zieht man die Gleichungen (72.) von (74.) ab, so erhält man

$$V_1 = U_1 - x_m u_{1,m};\quad V_2 = U_2 - x_m u_{2,m};\quad \dots\quad V_{m-1} = U_{m-1} - x_m u_{m-1,m}.$$

Setzt man diese Werthe von $V_1, V_2, \dots V_{m-1}$ in (75.), so findet sich:

$$\delta.x_1 = U_1 V_{1,1} + U_2 V_{2,1} + \dots U_{m-1} V_{m-1,1} - x_m\{u_{1,m} V_{1,1} + u_{2,m} V_{2,1} + \dots u_{m-1,m} V_{m-1,1}\},$$
$$\delta.x_2 = U_1 V_{1,2} + U_2 V_{2,2} + \dots U_{m-1} V_{m-1,2} - x_m\{u_{1,m} V_{1,2} + u_{2,m} V_{2,2} + \dots u_{m-1,m} V_{m-1,2}\},$$
$$\dots\dots\dots\dots\dots\dots$$
$$\delta.x_{m-1} = U_1 V_{1,m-1} + U_2 V_{2,m-1} + \dots U_{m-1} V_{m-1,m-1} - x_m\{u_{1,m} V_{1,m-1} + u_{2,m} V_{2,m-1} + \dots u_{m-1,m} V_{m-1,m-1}\}.$$

Multiplicirt man diese Gleichungen mit Δ, setzt darauf für $\Delta x_1, \Delta x_2, \dots \Delta x_m$ die Werthe aus (73.) und vergleicht die Coëfficienten von U_m auf beiden Seiten der Gleichungen, so ergiebt sich mit Rücksicht auf (76.):

$$U_{m,1} = -\{u_{1,m}V_{1,1} + u_{2,m}V_{2,1} + \dots + u_{m-1,m}V_{m-1,1}\},$$
$$U_{m,2} = -\{u_{1,m}V_{1,2} + u_{2,m}V_{2,2} + \dots + u_{m-1,m}V_{m-1,2}\},$$
$$\dots\dots\dots$$
$$U_{m,m-1} = -\{u_{1,m}V_{1,m-1} + u_{2,m}V_{2,m-1} + \dots + u_{m-1,m}V_{m-1,m-1}\}.$$

Mit Hülfe dieser Gleichungen stellt sich das vorhergehende System so dar:

$$\delta.x_1 = U_1V_{1,1} + U_2V_{2,1} + \dots + U_{m-1}V_{m-1,1} + x_mU_{m,1},$$
$$\delta.x_2 = U_1V_{1,2} + U_2V_{2,2} + \dots + U_{m-1}V_{m-1,2} + x_mU_{m,2},$$
$$\dots\dots\dots$$
$$\delta.x_m = U_1V_{1,m} + U_2V_{2,m-1} + \dots + U_{m-1}V_{m-1,m-1} + x_mU_{m,m-1},$$
$$\delta.x_m = U_mV_{m,m}.$$

Nimmt man nun an, dafs $u_{\varkappa,\lambda} = u_{\varkappa,\lambda}$, woraus bekanntlich folgt, dafs auch $U_{\varkappa,\lambda} = U_{\lambda,\varkappa}$ und $V_{\varkappa,\lambda} = V_{\lambda,\varkappa}$; so erhält man, wenn man respective mit U_1, U_2, ... U_m multiplicirt und alle Gleichungen addirt, mit Rücksicht auf die letzte Gleichung (73.):

$$77. \quad \delta.(x_1U_1 + x_2U_2 + \dots + x_mU_m) - x_mx_m\Delta$$
$$= U_1^2V_{1,1} + U_2^2V_{2,2} \dots U_{m-1}^2V_{m-1,m-1} + 2U_1U_2V_{1,2} + \dots + 2U_{m-2,m-1}V_{m-2,m-1}.$$

Es sei nun u eine gegebene Function $n$ten Grades der $m-1$ Variabeln x_1, x_2, ... x_{m-1}. Diese Function ist homogen und von m Variabeln, bleibt aber vom $n$ten Grade, wenn man $\frac{x_1}{x_m}$, $\frac{x_2}{x_m}$, ... $\frac{x_{m-1}}{x_m}$ statt der Variabeln setzt und die Function mit x_m^n multiplicirt. In dem Folgenden soll unter u die auf die angegebene Weise homogen gemachte Function u verstanden werden, mit der Bestimmung, dafs der Werth der letzten Variable x_m gleich 1 sei, wodurch die gegebene und die homogen gemachte Function gleich werden. Bezeichnet man ferner mit u_1, u_2, ... u_m die Differentialquotienten der homogenen Function u nach den m Variabeln genommen, so hat man bekanntlich:

$$78. \quad n.u = x_1u_1 + x_2u_2 + \dots x_mu_m.$$

Bezeichnet man endlich die zweiten Differentialquotienten der Function u, nämlich $\frac{\partial^2 u}{\partial x_\varkappa \partial x_\lambda}$, mit $u_{\varkappa,\lambda}$ oder $u_{\lambda,\varkappa}$, so hat man auf gleiche Weise:

$$79. \quad \begin{cases} n-1.u_1 = x_1u_{1,1} + x_2u_{1,2} + \dots + x_mu_{1,m}, \\ n-1.u_2 = x_1u_{2,1} + x_2u_{2,2} + \dots + x_mu_{2,m}, \\ \dots\dots\dots \\ n-1.u_m = x_1u_{m,1} + x_2u_{m,2} + \dots + x_mu_{m,m}. \end{cases}$$

Aus diesen Gleichungen erhellt, wenn man sie mit (72.) vergleicht, dafs

$$U_\varkappa = n-1.u_\varkappa$$

gesetzt werden kann; wodurch die Gleichung (77.) mit Rücksicht auf (78.) in

$$80. \quad n.\overline{n-1}.\delta.u - x_m.x_m.\Delta$$
$$= u_1^2 V_{1,1} + u_2^2 V_{2,2} + \ldots + u_{m-1}^2 V_{m-1,m-1} + 2u_1 u_2 V_{1,2} + \ldots + 2u_{m-2,m-1} V_{m-2,m-1}$$

übergeht. Diese Formel dient zur Transformation der Zähler der Ausdrücke (67.) und (71.); was sogleich erhellet, wenn man $m = 3$ oder $m = 4$ setzt.

26) Wenn man die Gleichungen (74.) unter der Annahme $m = 3$ auflöset, wodurch man die Gleichungen (75.) erhält, so ergiebt sich

$$V_{1,1} = u_{2,2}, \quad V_{2,2} = u_{1,1}, \quad V_{1,2} = -u_{1,2},$$

und die Determinante der Coëfficienten in den Gleichungen (72.) wird:

$$\Delta = u_{1,1}u_{2,2}u_{3,3} + 2u_{1,2}u_{1,3}u_{2,3} - u_{1,1}u_{2,3}^2 - u_{2,2}u_{1,3}^2 - u_{3,3}u_{1,2}^2.$$

Setzt man diese Werthe in die Gleichung (80.), so geht der Theil rechts derselben in den Zähler des Ausdrucks (67.) über. Bemerkt man nun, daſs die Coordinaten des Punctes p der Curve $u = 0$ die Function u verschwinden machen und daſs $x_3 = 1$ ist, so hat man:

$$67.^* \quad \lambda = \frac{-\Delta}{(n-1)^2(u_1^2 + u_2^2)}.$$

Für $m = 4$ wird.

$$V_{1,1} = u_{2,2}u_{3,3} - u_{2,3}^2, \quad V_{2,3} = u_{2,1}u_{3,1} - u_{1,1}u_{2,3}^2;$$
$$V_{2,2} = u_{3,3}u_{1,1} - u_{3,1}^2, \quad V_{3,1} = u_{3,2}u_{1,2} - u_{2,2}u_{3,1},$$
$$V_{3,3} = u_{1,1}u_{2,2} - u_{1,2}^2, \quad V_{1,2} = u_{1,3}u_{2,3} - u_{3,3}u_{1,2}.$$

Setzt man diese Werthe in den Theil rechts der Gleichung, so geht derselbe in den Zähler des Ausdrucks (71.) über, und da $x_4 = 1$ und für die Coordinaten des Punctes p der Oberfläche $u = 0$ die Function u verschwindet, so hat man:

$$71.^* \quad \lambda_1\lambda_2 = \frac{-\Delta}{(n-1)^2(u_1^2 + u_2^2 + u_3^2)}.$$

Diese Transformation ist vorzüglich deshalb von Wichtigkeit, weil sie die Grade der Zähler der Ausdrücke (67.) und (71.) um zwei Einheiten erniedrigt. Denn während der Zähler des Ausdrucks (67.) in Rücksicht auf die Variabeln vom Grade $3n-4$ war, so ist der Zähler des Ausdrucks (67.*) nur vom Grade $3(n-2)$. Ebenso ist der Zähler des Ausdrucks (71.) vom Grade $4n-6$, der Zähler des Ausdrucks (71.) aber nur vom $4(n-2)$ten Grade.

Man pflegt mit dem Namen Wendepuncte solche Puncte einer Curve zu bezeichnen, in denen der Krümmungshalbmesser unendlich groſs ist. Ist nun $u = 0$ die Gleichung einer Curve $n$ter Ordnung, so werden die Coordinaten dieser Puncte durch die Gleichungen

$$u = 0 \quad \text{und} \quad \lambda = 0$$

bestimmt. Nimmt man den Werth von λ aus (67.), so werden diese Gleichungen auf die Zahl der Wendepuncte gleich $n(3n-4)$ hindeuten. Setzt man aber für λ den Werth aus (67.*), so geht die letzte Gleichung in $\varDelta=0$ über und die Zahl der Wendepuncte reducirt sich auf $3n(n-2)$. Man hat daher folgenden von dem Herrn Professor *Plücker* in dem „System der analytischen Geometrie p. 264" aufgestellten Lehrsatz.

Lehrsatz 9.

Eine Curve $n$ter Ordnung hat im Allgemeinen $3n(n-2)$ Wendepuncte. Aus dem Vorhergehenden ergiebt sich folgende Regel zur Bestimmung der Wendepuncte: *Wenn u eine homogene Function von 3 Variabeln x_1, x_2, x_3 $n$ten Grades, $\varDelta$ die aus den zweiten partiellen Differentialquotienten zusammengesetzte Determinante der Function u ist, und $\frac{x_1}{x_3}$, $\frac{x_2}{x_3}$ sind die rechtwinkligen (oder schiefwinkligen) Coordinaten eines variabeln Punctes, so bestimmen die Gleichungen*

$$u=0 \quad \textit{und} \quad \varDelta=0$$

die Coordinaten der Wendepuncte der Curve $u=0$.

Nennt man auf gleiche Weise *Wendepuncte einer Oberfläche $u=0$* diejenigen Puncte, in denen einer der beiden Hauptschnitte der Oberfläche einen unendlich grofsen Krümmungsradius hat, so beweiset der Ausdruck (71.*), der für diese Puncte verschwinden mufs, nachstehenden Lehrsatz:

Lehrsatz 10.

Die Wendepuncte einer Oberfläche $n$ter Ordnung liegen auf einer Oberfläche $4(n-2)$ter Ordnung.

Zur Bestimmung dieser Art Wendepuncte dient folgende Angabe:

Wenn u eine homogene Function $n$ten Grades der 4 Variabeln x_1, x_2, x_3, x_4, $\varDelta$ die aus den zweiten partiellen Differentialquotienten zusammengesetzte Determinante der Function u ist, und $\frac{x_1}{x_4}$, $\frac{x_2}{x_4}$, $\frac{x_3}{x_4}$ sind die Coordinaten eines variabeln Punctes, so bestimmen die Gleichungen

$$u=0 \quad \textit{und} \quad \varDelta=0$$

die Coordinaten der Wendepuncte der Oberfläche $u=0$.

27) In No. 8. bis 14. sind mit f_1, f_2, f_3 beliebige homogene Functionen 2ten Grades von den Variabeln x_1, x_2, x_3 bezeichnet worden und mit φ die Determinante dieser Functionen. Betrachtet man die Quotienten $\frac{x_1}{x_3}$, $\frac{x_2}{x_3}$ als die rechtwinkligen Coordinaten eines Punctes der Ebene,

so stellen die Gleichungen

$$f_1 = 0, \quad f_2 = 0, \quad f_3 = 0$$

drei beliebige Kegelschnitte dar und die Gleichung $\varphi = 0$ eine Curve dritter Ordnung, die mit diesen Kegelschnitten in einem merkwürdigen Verhältnisse steht. Denn bezeichnet man mit $\frac{x_1}{x_3}$, $\frac{x_2}{x_3}$ die Coordinaten eines Punctes der Ebene und mit $\frac{y_1}{y_3}$, $\frac{y_2}{y_3}$ die Coordinaten des zugeordneten harmonischen Poles in Rücksicht auf jeden der erwähnten Kegelschnitte, so hat man, mit Beibehaltung der in den angegebenen Nummern gewählten Bezeichnungen, folgende Bedingungsgleichungen:

$$\begin{aligned} y_1 u_1^{(1)} + y_2 u_1^{(2)} + y_3 u_1^{(3)} &= 0, \\ y_1 u_2^{(1)} + y_2 u_2^{(2)} + y_3 u_2^{(3)} &= 0, \\ y_1 u_3^{(1)} + y_2 u_3^{(2)} + y_3 u_3^{(3)} &= 0. \end{aligned}$$

Das Resultat der Elimination von y_1, y_2, y_3 aus diesen Gleichungen giebt dann $\varphi = 0$; woraus folgender Lehrsatz hervorgeht.

Lehrsatz 11.

„Der geometrische Ort der dreien gegebenen Kegelschnitten gemeinschaftlichen zugeordneten harmonischen Polenpaare ist eine Curve dritter Ordnung."

Nimmt man an, dafs die drei gegebenen Kegelschnitte sich in einem und demselben Puncte schneiden, so wird in diesem eine Polenpaar zusammenfallen und deshalb die Curve dritter Ordnung durch diesen Punct hindurchgehen. Wenn man dies analytisch ausdrückt, so hat man den Lehrsatz 2.

Wenn man, anstatt von den Gleichungen $f_1 = 0$, $f_2 = 0$, $f_3 = 0$, von folgenden drei Gleichungen ausgegangen wäre:

$$\varkappa_1 f_1 + \varkappa_2 f_2 + \varkappa_3 f_3 = 0, \quad \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 = 0, \quad \mu_1 f_1 + \mu_2 f_2 + \mu_3 f_3 = 0,$$

so würde man dieselbe Endgleichung $\varphi = 0$ gefunden haben. Es stellt mithin die Gleichung $\varkappa_1 f_1 + \varkappa_2 f_2 + \varkappa_3 f_3 = 0$ ein System Kegelschnitte von der Eigenschaft dar, dafs sich, wenn man die gemeinsamen harmonischen Polenpaare von irgend dreien construirt, welche zugleich harmonische Polenpaare aller übrigen sind, immer dieselbe Curve dritter Ordnung als geometrischen Ort dieser Polenpaare ergiebt. Diese Curve dritter Ordnung läfst sich auf folgende Art construiren. Man lege einen beliebigen Kegelschnit durch die 4 Schnittpuncte der beiden ersten Kegelschnitte. Derselbe schneidet den dritten Kegelschnitt in 4 Puncten. Legt man alsdann durch die 4 letzten Schnittpuncte ein

Linienpaar, so laufen die beiden Linien in einem Puncte der Curve dritter Ordnung zusammen. Dieser Punct beschreibt die Curve dritter Ordnung, wenn man den beliebigen Kegelschnitt variiren läfst.

Umgekehrt läfst sich nach den drei Kegelschnitten fragen, deren gemeinschaftliche harmonische Polenpaare in einer gegebenen Curve dritter Ordnung liegen. Diese Aufgabe kommt mit der Aufgabe 1. überein. Denn wenn $\varphi = 0$ die Gleichung der gegebenen Curve dritter Ordnung ist, so hat man die Function f dritter Ordnung zu suchen, deren Determinante die gegebene Function φ ist. Hat man dieselbe bestimmt und bezeichnet nun mit f_1, f_2, f_3 ihre partiellen Differentialquotienten, so sind $f_1 = 0$, $f_2 = 0$, $f_3 = 0$ die Gleichungen der gesuchten Kegelschnitte, und die Gleichung $k_1 f_1 + k_2 f_2 + k_3 f_3 = 0$ stellt das ganze System von Kegelschnitten dar, deren gemeinschaftliche harmonische Polenpaare in der gegebenen Curve dritter Ordnung liegen. Da aber einer gegebenen Function φ drei Functionen f entsprechen, so giebt es auch drei Systeme solcher Kegelschnitte. Jedem Puncte der Curve entspricht ein zugeordneter Pol des Systems. Da aber 3 Systeme vorhanden sind, so entsprechen jedem Puncte der Curve drei andere bestimmte Puncte derselben Curve.

28) In No. 15. bis 22. ist mit f eine beliebige homogene Function dritter Ordnung von den Variabeln x_1, x_2, x_3, und mit φ ihre Determinante bezeichnet worden. Aus dem Vorgehenden erhellet, dafs die Gleichungen

$$f = 0 \quad \text{und} \quad \varphi = 0,$$

die Wendepuncte der durch die Gleichung $f = 0$ dargestellten Curve dritter Ordnung bestimmen. Bemerkt man nun, dafs, wenn mit d und δ zwei beliebige constante Gröfsen bezeichnet werden, die Gleichung $df + \delta\varphi = 0$ alle Curven dritter Ordnung darstellt, welche durch die Wendepuncte der ersten Curve hindurchgehen, so lassen sich die Lehrsätze 8. und 6. wie folgt geometrisch ausdrücken.

Lehrsatz 12.

Durch die 9 Wendepuncte einer beliebigen Curve dritter Ordnung lassen sich 4 Systeme dreier geraden Linien hindurchlegen.

Auf diesen schönen Lehrsatz hat zuerst Herr Professor *Plücker* in der oben citirten Schrift S. 284 aufmerksam gemacht. Die Schnittpuncte eines beliebigen dieser Systeme mit einem der drei andern werden demnach die Wendepuncte der Curve dritter Ordnung sein.

Lehrsatz 13.

Alle Curven dritter Ordnung, welche durch die 9 Wendepuncte einer beliebigen Curve dritter Ordnung hindurchgehen, schneiden sich gegenseitig in den Wendepuncten.

Hieran schliefst sich endlich noch folgender Lehrsatz, der ebenfalls durch das Vorhergehende bewiesen wird.

Lehrsatz 14.

Wenn die Wendepuncte zweier Curven dritter Ordnung auf denselben drei geraden Linien liegen, so liegen auch die Wendepuncte aller Curven dritter Ordnung, welche durch sämmtliche Schnittpuncte der beiden Curven hindurchgehen, auf denselben drei geraden Linien.

Die Gleichungen des einen Systems von 3 geraden Linien, welche durch die 9 Wendepuncte der Curve $f=0$ hindurchgehen, sind, wie aus der Gleichung (57.) erhellet:

$$y_1 = 0, \quad y_2 = 0, \quad y_3 = 0.$$

Die eines zweiten Systems sind

$$z_1 = 0, \quad z_2 = 0, \quad z_3 = 0,$$

wo die Werthe von z_1, z_2, z_3 aus einer der drei Substitutionen von No. 22. und die Werthe von y_1, y_2, y_3 aus den Substitutionen (53.) zu nehmen sind. Jede von den drei Linien des ersten Systems schneidet jede Linie des andern Systems in einem Wendepuncte der Curve $f=0$. Berechnet man daher die Werthe der Verhältnisse der Variabeln x_1, x_2, x_3 aus irgend einem Paare folgender Gleichungen:

$$\begin{array}{lll} y_1=0,\ y_2+y_3=0; & y_2=0,\ y_3+y_1=0; & y_3=0,\ y_1+y_2=0; \\ y_1=0,\ y_2+k'y_3=0; & y_2=0,\ y_3+k'y_1=0; & y_3=0,\ y_1+k'y_2=0; \\ y_1=0,\ y_2+k''y_3=0; & y_2=0,\ y_3+k''y_1=0; & y_3=0,\ y_1+k''y_2=0; \end{array}$$

so werden diese Werthe der Verhältnisse der Variabeln auch den Gleichungen

$$f=0 \quad \text{und} \quad \varphi=0$$

genügen und die Quotienten $\frac{x_1}{x_3}$, $\frac{x_2}{x_3}$ die Coordinaten eines Wendepunctes der durch $f=0$ dargestellten Curve dritter Ordnung sein.

Königsberg, den 22. April 1844.

12.

Allgemeine Berechnung der fünf regulären Körper.

(Von Herrn *F. Schultze*, Privatlehrer zu Berlin.)

Bezeichnet man *den Inhalt des Körpers* mit K, *den Inhalt jeder seiner Seitenflächen* mit F, *deren Anzahl* mit n und *das Maafs des Halbmessers der in den Körper beschriebenen Kugel* mit ϱ: so ist

$$1. \quad K = \tfrac{1}{3} n F \varrho.$$

Bezeichnet man ferner *die Anzahl der Seiten jeder Seitenfläche* mit n' und *das Maafs jeder Kante* mit s, so ist

$$2. \quad F = n'.(\tfrac{1}{2}s)^2.\cot\frac{180^\circ}{n'}.$$

Bezeichnet man nun *das Maafs des Halbmessers der um den Körper beschriebenen Kugel* mit r und *das Maafs des Halbmessers des um jede Seitenfläche beschriebenen Kreises mit* $\mathfrak{r}$: so ist

$$3. \quad r^2 = \varrho^2 + \mathfrak{r}^2.$$

Bezeichnet man alsdann *das Maafs des Winkels, welchen zwei aus den Endpuncten einer Kante gezogene Halbmesser mit einander bilden,* mit μ, so ist

$$4. \quad r = \tfrac{1}{2} s \operatorname{cosec} \tfrac{1}{2}\mu.$$

Stellt man sich nun auf der Oberfläche der um den Körper beschriebenen Kugel die Ecken des Körpers durch Meridianbogen verbunden, die ganze Kugel-Oberfläche also hierdurch in ein Netz von n regulären sphärischen n'ecken zerlegt vor; alsdann den Pol (P) eines derselben (es möge dasselbe ein reguläres Fünfeck $ABCDE$ sein) mit seinen Ecken gleichfalls durch Meridianbogen (PA, PB, PC, PD, PE) verbunden und in einem der auf diese Weise entstehenden sphärischen Dreiecke (etwa in APE) vom Pol (P) aus senkrecht auf die gegenüberliegende Seite (AE) einen Meridianbogen (PF) gezogen, und bezeichnet *das Maafs jedes Winkels der sphärischen* n'*ecke* mit A, *das Maafs jedes der* n' *um den Pol* (P) *liegenden sphärischen Winkel* aber mit M: so ist (in dem rechtwinkligen sphärischen Dreieck AFP oder EFP)

$$5. \quad \cos\tfrac{1}{2}M = \cos\tfrac{1}{2}\mu \sin\tfrac{1}{2}A.$$

Nun ist

$$n'.M = 360°,$$

folglich

$$6. \quad M = \frac{360°}{n'},$$

und ferner, wenn *die Anzahl der Kanten jeder Ecke des Körpers* mit n'' bezeichnet wird,

$$n''.A = 360°,$$

also

$$7. \quad A = \frac{360°}{n''};$$

folglich ist aus (5. 6. und 7.)

$$\cos\frac{180°}{n'} = \cos\tfrac{1}{2}\mu \sin\frac{180°}{n''}$$

und hieraus

$$8. \quad \cos\tfrac{1}{2}\mu = \frac{\cos\frac{180°}{n'}}{\sin\frac{180°}{n''}}.$$

Es ist aber

$$\operatorname{cosec}\tfrac{1}{2}\mu = \frac{1}{\sqrt{(1-(\cos\frac{1}{2}\mu)^2)}}$$

und, wenn hierin für $\cos\frac{1}{2}\mu$ aus (8.) sein Werth *substituirt* wird,

$$\operatorname{cosec}\tfrac{1}{2}\mu = \frac{1}{\sqrt{\left(1-\left(\frac{\cos\frac{180°}{n'}}{\sin\frac{180°}{n''}}\right)^2\right)}}$$

oder

$$9. \quad \operatorname{cosec}\tfrac{1}{2}\mu = \frac{\sin\frac{180°}{n''}}{\sqrt{\left(\left(\sin\frac{180°}{n''}\right)^2-\left(\cos\frac{180°}{n'}\right)^2\right)}};$$

desgleichen ist alsdann aus (4. und 9.)

$$10. \quad r = \tfrac{1}{2}s.\frac{\sin\frac{180°}{n''}}{\sqrt{\left(\left(\sin\frac{180°}{n''}\right)^2-\left(\cos\frac{180°}{n'}\right)^2\right)}}.$$

Es ist ferner

$$11. \quad r = \tfrac{1}{2}s \operatorname{cosec}\frac{180°}{n'},$$

folglich aus (3. 10. und 11.)

$$\left(\tfrac{1}{2}s.\frac{\sin\frac{180^\circ}{n''}}{\sqrt{\left(\left(\sin\frac{180^\circ}{n''}\right)^2-\left(\cos\frac{180^\circ}{n'}\right)^2\right)}}\right)^2=\varrho^2+\left(\tfrac{1}{2}s.\operatorname{cosec}\frac{180^\circ}{n'}\right)^2$$

und hieraus

$$12.\qquad \varrho=\tfrac{1}{2}s.\frac{\cot\frac{180^\circ}{n'}\cos\frac{180^\circ}{n''}}{\sqrt{\left(\left(\sin\frac{180^\circ}{n''}\right)^2-\left(\cos\frac{180^\circ}{n'}\right)^2\right)}};$$

endlich ist aus (1. 2. und 12.)

$$(\mathrm{I.})\quad K=\tfrac{1}{3}nn'.(\tfrac{1}{2}s)^3.\frac{\left(\cot\frac{180^\circ}{n'}\right)^2\cos\frac{180^\circ}{n''}}{\sqrt{\left(\left(\sin\frac{180^\circ}{n''}\right)^2-\left(\cos\frac{180^\circ}{n'}\right)^2\right)}}.$$

Eliminirt man aus dieser Gleichung s mit Hülfe der Gleichungen (10. und 12.), so erhält man noch

$$(\mathrm{II.})\quad K=\tfrac{1}{3}nn'.r^3.\left(\left(\sin\frac{180^\circ}{n''}\right)^2-\left(\cos\frac{180^\circ}{n'}\right)^2\right)\left(\cot\frac{180^\circ}{n'}\right)^2\cot\frac{180^\circ}{n''}\left(\operatorname{cosec}\frac{180^\circ}{n''}\right)^2$$

und

$$(\mathrm{III.})\quad K=\tfrac{1}{3}nn'.\varrho^3.\left(\left(\sin\frac{180^\circ}{n''}\right)^2-\left(\cos\frac{180^\circ}{n'}\right)^2\right)\operatorname{tang}\frac{180^\circ}{n'}\left(\sec\frac{180^\circ}{n''}\right)^2$$

13.
Encyklopädische und elementare Darstellung der Theorie der Zahlen.

(Vom Herausgeber dieses Journals.)

(Fortsetzung der Abhandlung No. 2. im 1ten, No. 10. im 2ten und No. 26. im 3ten Hefte sieben und zwanzigsten Bandes.)

---

§. 57.
Erklärung.

Zufolge (§. 56.) giebt es, wenn p eine *Stammzahl* ist, immer Werthe von $z > 1$, von welchen schon *niedrigere* Potenzen, als nach dem Fermatschen Satze die Potenz z^{p-1}, zu p den Rest 1 lassen, also immer *Wurzeln* > 1 zu der Gleichung

$$1.\quad z^{\varepsilon} = \mathfrak{G}p + 1,$$

wo $\varepsilon < p - 1$.

Nun giebt es auch offenbar immer *niedrigste* Exponenten λ, für welche, für bestimmte z,

$$2.\quad z^{\lambda} = \mathfrak{G}p + 1$$

ist.

Die Wurzeln z *dieser* Gleichung, für den *niedrigsten* Exponenten λ, die also für alle *kleineren* Exponenten 1, 2, 3, ... bis $\lambda - 1$ *andere* Reste als 1 und *zuerst* für den Exponenten λ den Rest 1 geben, sollen *Stammwurzeln aus* 1 *zu* p *für den Exponenten* λ, oder kürzer, λ*te Stammwurzeln aus* 1 *zu* p heifsen und durch z_{λ} bezeichnet werden.

Ist λ gleich $p - 1$ selbst, so dafs also *alle niedrigere* Potenzen als z^{p-1} andere Reste als 1 zu p lassen, so sollen die z, welche diese Eigenschaft haben, *Hauptstammwurzeln aus* 1 *zu* p heifsen.

Gewöhnlich giebt man nur den *Hauptstammwurzeln* einen besondern Namen; man nennt sie *primitive Wurzeln.* Es ist aber gut, auch den übrigen Stammwurzeln, für welche $\varepsilon < p - 1$ ist, eine besondere Benennung beizulegen; und die Benennungen *Stammwurzel,* und für den Fall $\varepsilon = p - 1$ *Hauptstammwurzel,* scheinen passend, wenigstens nicht minder passend zu sein, als die nicht deutsche Benennung für letztere.

Wenn in der Gleichung

$$3.\quad z^{x} = \mathfrak{G}p + r$$

z eine *Hauptstammwurzel* und $x < p - 1$, also r zufolge der Eigenschaft der Stammwurzeln *nicht* $= 1$ ist, so nennt man auch den Exponenten x, für welchen der Rest r Statt findet, *Index* zu r.

§. 58.

Lehrsatz.

I. *Es giebt, wenn* p *eine Stammzahl ist, zu jedem Exponenten* $\delta > 1$, *der in* $p-1$ *aufgeht, also auch zu* $p-1$ *selbst, Stammwurzeln; das heifst Werthe von* z, *von welchen keine niedrigere Potenz als* z^δ *zu* p *den Rest* 1 *läfst, also für welche für keinen kleineren Exponenten als* δ

$$1.\quad z^\delta = \mathfrak{G}p+1$$

ist.

II. *Zu Exponenten* δ, *die nicht in* $p-1$ *aufgehen, gleichviel ob sie mit* $p-1$ *Theiler gemein haben, oder nicht, giebt es keine Stammwurzeln.*

Beispiel. (Aus Taf. I.) $z=1$, 13 und 47 sind die *Stammwurzeln* zu dem Theiler $\delta=4$ von $p-1=60$. $z=3, 27, 41$ und 52 sind die *Stammwurzeln* zu dem Theiler $\delta=10$ von $p-1$, und $z=8, 23, 24, 28, 33, 37, 38$ und 53 sind die *Stammwurzeln* zu dem Theiler $\delta=20$ von $p-1$ u. s. w. $z=2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55$ und 59 sind die *Hauptstammwurzeln* oder diejenigen zu $\delta=p-1=60$.

Beweis von I. *A.* Nach (§. 56. III.) giebt es für jeden Theiler δ von $p-1$, δ verschiedene Werthe von z, so wie nach (§. 40.) für δ *gleich* $p-1$, $p-1$ verschiedene Werthe von z, für welche

$$2.\quad z^\delta = \mathfrak{G}p+1$$

ist.

B. Giebt nun in der Gleichung (2.) keine der verschiedenen Potenzen $z^1, z^2, z^3, \ldots, z^{\delta-1}$ zu p den Rest 1, sondern erst z^δ selbst, so ist z in (2.) *selbst* die δte *Stammwurzel* aus 1 zu p.

Geben aber schon niedrigere Potenzen als z^δ zu p den Rest 1, so wird nothwendig irgend eine derselben die *niedrigste* sein. Man setze, ihr Exponent sei $=\lambda$. Alsdann ist zunächst zu zeigen, dafs λ ein *Theiler* von δ und folglich von $p-1$ sein mufs.

C. Gesetzt λ sei *nicht* ein Theiler von δ, also

$$3.\quad \delta = \mathfrak{G}\lambda+\varrho,$$

wo $\varrho > 0$ und $< \lambda$ ist, so müfste, da

$$4.\quad z^\lambda = \mathfrak{G}p+1$$

vorausgesetzt wird, nach (2. und 3.)

$$5.\quad z^\delta = z^{\mathfrak{G}\lambda+\varrho} = z^{\mathfrak{G}\lambda}z^\varrho = \mathfrak{G}p+1,$$

oder, da nach (4.) $z^{\mathfrak{G}\lambda} = (\mathfrak{G}p+1)^{\mathfrak{G}} = \mathfrak{G}p+1$ ist (5.),

$$(\mathfrak{S}p+1)z^{\varrho} = \mathfrak{S}p+1 \text{ oder}$$

$$6. \quad z^{\varrho} = \mathfrak{S}p+1$$

sein; also müfste, da $\varrho < \lambda$ ist, eine *noch niedrigere* Potenz als z^{λ} zu p den Rest 1 lassen. Da dieses gegen die Voraussetzung ist, so kann nicht $\delta = \mathfrak{S}\lambda+\varrho$, sondern nur $\delta = \mathfrak{S}\lambda$ und folglich λ nur ein *Theiler* von δ sein.

D. Nun ist nothwendig jeder Theiler λ von δ ein Theiler von $p-1$ selbst. Und da es nun für *jeden* Theiler λ von $p-1$, so wie für $\lambda = p-1$ selbst, Werthe von z giebt, die der Gleichung $z^{\lambda} = \mathfrak{S}p+1$ genugthun, so giebt es auch für jeden Theiler λ oder δ von $p-1$ *Stammwurzeln.*

Beweis von II. *E.* Ist δ zu $p-1$ *theilerfremd,* so bekommt nach (§. 56. II.) in

$$7. \quad z^{\delta} = \mathfrak{S}p+r$$

r für jeden Werth von z einen *andern* Werth und die Werthe von r durchlaufen alle die Zahlen $1, 2, 3, 4, \ldots. p-1$. Also ist kein r, aufser für $z=1$, gleich 1; mithin findet die Gleichung (1.) nur allein für $z=1$ Statt, und folglich giebt es in diesem Fall *keine* Stammwurzeln.

F. Hat δ mit $p-1$ einen Theiler λ gemein, so dafs z. B.

$$8. \quad \delta = \lambda\eta \quad \text{und} \quad p-1 = \lambda\tau$$

ist, so giebt es schon für den *kleinsten* Theiler λ von δ Stammwurzeln; denn es giebt deren nach (1.) für *jeden* Exponenten, welcher, wie λ, ein Theiler von $p-1$ ist. Also ist schon

$$9. \quad z^{\lambda} = \mathfrak{S}p+1,$$

während *zugleich*

$$10. \quad z^{\delta} = z^{\lambda\eta} = (\mathfrak{S}p+1)^{\eta} = \mathfrak{S}p+1$$

ist, und die z, welche der Gleichung (10.) oder (1.) entsprechen, sind nicht mehr *Stammwurzeln* aus 1, weil schon die *niedrigere* Potenz z^{λ} von z den Rest 1 läfst. Mithin giebt es auch in diesem Fall keine *Stammwurzeln* aus 1 zu p, und folglich überhaupt, wenn δ nicht in $p-1$ *aufgeht,* keine δten Stammwurzeln aus 1 zu p; gemäfs (II.).

Anm. *G.* Der Satz geht insbesondere aus (§. 56.) hervor.

§. 59.

Lehrsatz.

Wenn in der Zahlengleichung

$$1. \quad z_{\delta}^{\delta} = \mathfrak{S}p+1$$

p *eine Stammzahl,* δ *ein Theiler von* $p-1$ *und* z_{δ} *einer der* δ*ten Stammwurzeln aus* 1 *zu* p *ist, so sind*

I. *Die Reste zu allen den Potenzen* $z_\delta^1, z_\delta^2, z_\delta^3, z_\delta^4, \ldots z_\delta^\delta$ *von* z *unter einander verschieden, und wenn man die weitern, höheren Potenzen nimmt, so kehren dieselben Reste in derselben Ordnung wieder, und bilden also eine Periode. Das heifst, in Zeichen ausgedrückt: wenn man in der Gleichung*

$$2.\quad z_\delta^{n\delta+x} = \mathfrak{G}p + r_{n\delta+x}$$

der Reihe nach

$$3.\quad x = 1, 2, 3, \ldots \delta \quad \text{und} \quad n = 0, 1, 2, 3, \ldots \left(\frac{p-1}{\delta} - 1\right)$$

setzt, so sind die r, *welche sich in* (2.) *ergeben, für ein und dasselbe* n *unter einander verschieden, für gleiche* x *und verschiedene* n *aber einander gleich, so dafs*

$$4.\quad r_{n\delta+x} = r_x.$$

II. *Ist in* (I.) z *eine Hauptstammwurzel, also* $\delta = p-1$, *so durchläuft, wenn man in*

$$5.\quad z_{p-1}^x = \mathfrak{G}p + r$$

der Reihe nach

$$6.\quad x = 1, 2, 3, \ldots p-1$$

setzt, r *ebenfalls alle die Zahlen* $1, 2, 3, \ldots p-1$; *nur in anderer Ordnung als* z.

Beispiele. (Aus Taf. I.) Zu I. Für die $\delta = 3$te *Stammwurzel* 13 ist die immerfort wiederkehrende Periode der Reste zu z^1, z^2, z^3 etc. 13, 7 und 1. Für die $\delta = 4$te *Stammwurzel* 50 ist die Periode zu z^1, z^2, z^3, z^4 etc. 50, 60, 11 und 1. Für die $\delta = 10$te *Stammwurzel* 3 ist die Periode der Reste zu z^1, z^2, z^3, ... z^{10} etc. 3, 9, 27, 20, 60, 58, 52, 34, 41 und 1. U. s. w. Immer sind die Reste in jeder Periode *unter sich verschieden.*

Zu II. Für die *Hauptstammwurzel* 2 z. B. durchlauft r alle die Zahlen 1, 2, 3, 4, ... 60, obwohl in verschiedener Ordnung von x. Eben so verhält sich für die andern *Hauptstammwurzeln* 6, 7, 10, 17 etc.

Beweis *A*. Die Gleichung (2.) ist so viel als

$$7.\quad z^{n\delta} z^x = \mathfrak{G}p + r_{n\delta+x}$$

und, da vermöge (1.) $z^{n\delta} = (\mathfrak{G}p+1)^n = \mathfrak{G}p+1$ ist, so viel als

$$(\mathfrak{G}p+1)z^x = \mathfrak{G}p + r_{n\delta+x} \text{ oder}$$

$$8.\quad z^x = \mathfrak{G}p + r_{n\delta+x}.$$

Nun ist auch nach (2.)

$$9.\quad z^x = \mathfrak{G}p + r_x,$$

also folgt aus (8. und 9.)

$$\mathfrak{S}p + r_{n\delta+x} = \mathfrak{S}p + r_x \text{ oder}$$

$$10. \quad r_{n\delta+x} = \mathfrak{S}p + r_x$$

und, da beide $r < p$ sein sollen,

$$11. \quad r_{n\delta+x} = r_x;$$

gemäfs (4.).

B. Gäben nun z. B.: z^{x_1} und z^{x_2} *gleiche* Reste $r_{x_1} = r_{x_2}$, so wäre

$$12. \quad z^{x_1} = \mathfrak{S}p + r_{x_1} \quad \text{und} \quad z^{x_2} = \mathfrak{S}p + r_{x_2},$$

also

$$13. \quad z^{x_1} - z^{x_2} = \mathfrak{S}p,$$

oder, wenn von den beiden Zahlen x_1 und x_2 etwa x_1 die *gröfsere* ist,

$$14. \quad z^{x_2}(z^{x_1-x_2} - 1) = \mathfrak{S}p.$$

Da $z < p$ ist, so geht z und folglich z^{x_2} mit p *nicht* auf, also müfste, zufolge (14.), $z^{x_1-x_2} - 1$ mit p *aufgehen*, mithin

$$15. \quad z^{x_1-x_2} = \mathfrak{S}p + 1$$

sein. Aber x_1 und x_2 sind nicht gröfser als δ, wiewohl > 0, also ist $x_1 - x_2 < \delta$: folglich gäbe nach (15.) schon eine *niedrigere* Potenz als z^δ zu p den Rest 1. Dies ist der Voraussetzung entgegen, da z eine *Stammwurzel* sein soll. Also können die Potenzen einer *Stammwurzel* z mit Exponenten $< \delta$ nicht *gleiche* Reste r zu p lassen, und folglich sind die Reste zu allen den Potenzen $z^1, z^2, z^3, z^4, \ldots z^\delta$ unter einander *verschieden.*

Dieses zusammen ist was (I.) behauptet.

C. Da nach (I.) für *jede Stammwurzel*, also auch für die *Hauptstammwurzeln*, alle Reste r in (5.) unter sich verschieden sind, wenn man $x = 1, 2, 3, \ldots p-1$ setzt, die *Anzahl* der verschiedenen Reste aber so grofs ist, als die der Werthe von x, folglich $= p-1$, und dabei alle $r < p$ sind, so sind die Werthe von r in (5.) nothwendig alle die Zahlen 1, 2, 3, ... $p-1$ selbst. Und zwar sind sie es nothwendig in *anderer* Ordnung als x; denn wenn z. B. für ein *bestimmtes* x, $z^x = \mathfrak{S}p + r$ ist, so ist *nicht* für $x+1$, $z^{x+1} = \mathfrak{S}p + r + 1$, sondern z^{x+1} oder $z^x.z = (\mathfrak{S}p + r)z = \mathfrak{S}p + rz$, und rz kann nicht $= r+1$ sein, da alle r für die *Haupt*stammwurzeln > 1 sind, bis auf das letzte r zu z^{p-1}, also für $x = p-1$, welches, als das höchste x, das *letzte* ist.

I. *Die Reste zu allen den Potenzen* $z_\delta^1, z_\delta^2, z_\delta^3, z_\delta^4, \ldots z_\delta^\delta$ *von* z *unter einander verschieden, und wenn man die weitern, höheren Potenzen nimmt, so kehren dieselben Reste in derselben Ordnung wieder, und bilden also eine Periode. Das heifst, in Zeichen ausgedrückt: wenn man in der Gleichung*

$$2. \quad z_\delta^{n\delta+\varkappa} = \mathfrak{G}p + r_{n\delta+\varkappa}$$

der Reihe nach

$$3. \quad \varkappa = 1, 2, 3, \ldots \delta \quad \text{und} \quad n = 0, 1, 2, 3, \ldots \left(\frac{p-1}{\delta} - 1\right)$$

setzt, so sind die r, *welche sich in* (2.) *ergeben, für ein und dasselbe* n *unter einander verschieden, für gleiche* $\varkappa$ *und verschiedene* n *aber einander gleich, so dafs*

$$4. \quad r_{n\delta+\varkappa} = r_\varkappa.$$

II. *Ist in* (1.) z *eine Hauptstammwurzel, also* $\delta = p - 1$, *so durchläuft, wenn man in*

$$5. \quad z_{p-1}^\varkappa = \mathfrak{G}p + r$$

der Reihe nach

$$6. \quad \varkappa = 1, 2, 3, \ldots p - 1$$

setzt, r *ebenfalls alle die Zahlen* 1, 2, 3, ... p — 1; *nur in anderer Ordnung als* z.

Beispiele. (Aus Taf. I.) Zu I. Für die $\delta = 3$te *Stammwurzel* 13 ist die immerfort wiederkehrende Periode der Reste zu z^1, z^2, z^3 etc. 13, 7 und 1. Für die $\delta = 4$te *Stammwurzel* 50 ist die Periode zu z^1, z^2, z^3, z^4 etc. 50, 60, 11 und 1. Für die $\delta = 10$te *Stammwurzel* 3 ist die Periode der Reste zu $z^1, z^2, z^3, \ldots z^{10}$ etc. 3, 9, 27, 20, 60, 58, 52, 34, 41 und 1. U. s. w. Immer sind die Reste in jeder Periode *unter sich verschieden.*

Zu II. Für die *Hauptstammwurzel* 2 z. B. durchläuft *r* alle die Zahlen 1, 2, 3, 4, ... 60, obwohl in verschiedener Ordnung von $\varkappa$. Eben so verhält sich für die andern *Hauptstammwurzeln* 6, 7, 10, 17 etc.

Beweis *A.* Die Gleichung (2.) ist so viel als

$$7. \quad z^{n\delta} z^\varkappa = \mathfrak{G}p + r_{n\delta+\varkappa}$$

und, da vermöge (1.) $z^{n\delta} = (\mathfrak{G}p + 1)^n = \mathfrak{G}p + 1$ ist, so viel als

$$(\mathfrak{G}p + 1) z^\varkappa = \mathfrak{G}p + r_{n\delta+\varkappa} \quad \text{oder}$$

$$8. \quad z^\varkappa = \mathfrak{G}p + r_{n\delta+\varkappa}.$$

Nun ist auch nach (2.)

$$9. \quad z^\varkappa = \mathfrak{G}p + r_\varkappa,$$



Beweis A. Man setze

$$4.\quad \delta = \mu\lambda \text{ und } \varkappa = \nu\lambda,$$

wo λ den ***gröfsten Gemeintheiler*** von $\varkappa$ und δ bezeichnet. Nimmt man nun in (1.) die $\frac{\delta}{\lambda} = \mu$te Potenz, so ergiebt sich

$$5.\quad \mathfrak{z}^{\mu\varkappa} = \mathfrak{G}p + r_\varkappa^\mu$$

oder, gemäfs (4.),

$$6.\quad \mathfrak{z}^{\frac{\delta}{\lambda}\cdot\nu\lambda} = \mathfrak{z}^{\delta\nu} = \mathfrak{G}p + r_\varkappa^\mu,$$

oder, da nach (1.)

$$7.\quad \mathfrak{z}^{\nu\delta} = (\mathfrak{G}p+1)^\nu = \mathfrak{G}p+1$$

ist,

$$\mathfrak{G}p+1 = \mathfrak{G}p + r_\varkappa^\mu \text{ oder}$$

$$8.\quad r_\varkappa^\mu = \mathfrak{G}p+1 = r_\varkappa^{\frac{\delta}{\lambda}}$$

Also läfst die $\mu = \frac{\delta}{\lambda}$te Potenz von $r_\varkappa$ zu p den Rest 1.

B. Aber keine ***niedrigere*** als die $\mu = \frac{\delta}{\lambda}$te Potenz von $r_\varkappa$ kann den Rest 1 lassen; denn wäre es so, so müfste in (8.) λ ein anderer Theiler λ_1 von δ sein, der ***gröfser*** ist als der ***gröfste Gemeintheiler*** λ von δ und $\varkappa$. Ein ***Theiler*** von δ müfste λ_1 ***immer*** sein, weil sonst $\frac{\delta}{\lambda_1}$ keine ***ganze*** Zahl wäre. Es wäre aber für einen solchen Theiler λ_1 in (4.) ν keine ***ganze*** Zahl, da vorausgesetzt ist, dafs λ der ***gröfste*** Gemeintheiler von δ und $\varkappa$ sein soll. Nun könnte zwar $\nu\delta$ in (7.), auch wenn ν ein Bruch ist, immer noch eine ***ganze*** Zahl sein, aber diese Zahl wäre dann kein ***ganzzahliges Vielfache*** von δ, sondern etwa $= n\delta + \varrho$, wo $\varrho > 0$ und $< \delta$ ist. Solche Potenzen von $\mathfrak{z}$ in (7.) lassen aber zu p ***nicht*** den Rest 1, sondern nach (§. 59. I.) lauter unter einander von 1 ***verschiedene*** Reste. Also kann λ ***nicht gröfser*** sein als der ***gröfste Gemeintheiler*** von δ und $\varkappa$, und folglich läfst in (8.) keine ***kleinere*** als die $\frac{\delta}{\lambda} = \mu$te Potenz von $r_\varkappa$ den Rest 1 zu p, mithin ist $r_\varkappa$ in (8.) eine $\frac{\delta}{\lambda}$te ***Stammwurzel*** aus 1 zu p, und ***jedes*** r, welches die Gleichung (1.) für die verschiedenen Werthe von $\varkappa$ giebt, deren ***gröfster Gemeintheiler*** mit δ gleich λ ist, ist eine ***solche.***

C. Es kann aber auch ***kein anderes*** r als diejenigen, welche die Gleichung (1.) giebt, eine $\frac{\delta}{\lambda}$te Stammwurzel aus 1 zu p sein. Denn die

Gleichung (1.) giebt *alle* r, für welche δ und x die Zahl λ zum gröfsten Gemeintheiler hat. *Andere* r müfsten also Werthen von x entsprechen, die mit δ *andere* gröfste Gemeintheiler λ_1 hätten, und diese sind dann nach (*B.*) nicht mehr $\frac{\delta}{\lambda}$te, sondern $\frac{\delta}{\lambda_1}$te, also *andere* Stammwurzeln aus 1 zu p. Also sind die r in (1.) *alle* $\frac{\delta}{\lambda}$te Stammwurzeln aus 1 zu p, und es giebt *keine anderen* eiter.

Dieses zusammen ist was (I.) behauptet.

D. Haben δ und x in (1.) *keinen* Theiler $\lambda > 1$ gemein, so ist ihr *gröfster Gemeintheiler* $\lambda = 1$, und folglich in (4.) $\mu = \delta$, also dann in (8.)

$$9. \quad r_x^\delta = \mathfrak{G}p + 1.$$

Folglich sind dann die r_x in (1.) alle die δten *Stammwurzeln* x aus 1 zu p selbst; gemäfs (II.).

§. 61.

Lehrsatz.

I. *Von den verschiedenen* δ*ten Stammwurzeln aus* 1 *zu der Stammzahl* p *geben die* 1*te,* 2*te,* 3*te,* 4*te,* .... δ*te Potenzen gleichmäfsig, obwohl in verschiedener Ordnung, immer dieselben Reste zu* p, *unter welchen dann nach* (§. 60. II.) *auch die Werthe von* z *selbst sind; so dafs also für jede der verschiedenen Stammwurzeln* z_δ *in der Gleichung*

$$1. \quad z^\delta = \mathfrak{G}p + 1,$$

wo δ *ein Theiler von* $p-1$ *ist, wenn man in*

$$2. \quad z^\varepsilon = \mathfrak{G}p + r_\varepsilon$$

der Reihe nach

$$3. \quad \varepsilon = 1, 2, 3, 4, \ldots . \delta$$

setzt, r_ε *immer dieselben Zahlen durchlauft, unter denen sich auch die Werthe von* z *selbst befinden, jedoch für jeden andern Werth von* z *in verschiedener Ordnung.*

II. *Die Ordnung der Aufeinanderfolge der Reste für irgend eine* δ*te Stammwurzel* z_2 *wird durch die Aufeinanderfolge der Reste für eine andere* δ*te Stammwurzel* z_1 *dadurch bestimmt, dafs, wenn z. B.*

$$4. \quad z_1^x = \mathfrak{G}p + z_2$$

ist und man setzt

$$5. \quad z_1^\varepsilon = \mathfrak{G}p + r_\varepsilon,$$

$$6. \quad \varepsilon x = n\delta + x_1, \text{ wo } x_1 < \delta \text{ *und*}$$

$$7. \quad z_1^{x_1} = \mathfrak{G}p + r_{x_1}:$$

dafs alsdann in (5. *und* 7.)

$$8. \quad r_\varepsilon = r_{x_1}$$

ist, das heifst, dafs $z_1^{\varepsilon x}$ *und* z_2^ε *zu* p *gleiche Reste* r_ε *und* r_{x_1} *lassen, so dafs folglich für je zwei Werthe* z_1 *und* z_2 *von* z_δ, *welche die Gleichung* (4.) *erfüllen,*

$$9. \quad \left\{\begin{matrix} z_1^x, & z_1^{2x}, & z_1^{3x}, & z_1^{4x}, & \dots & z_1^{\delta x} \\ \textit{und } z_2^1, & z_2^2, & z_2^3, & z_2^4, & \dots & z_2^\delta \end{matrix}\right\} \text{ *zu* p *gleiche Reste lassen.*}$$

Beispiel. (Aus Taf. I.) Zu I. Die $\delta = 10$te Stammwurzeln für $p = 61$ sind nach der Tafel 3, 27, 41, 52, und die 1te, 2te, 3te, 4te, ... 10 ($=\delta$)te Potenzen dieser *verschiedenen* Stammwurzeln geben zu p gleichmäfsig *dieselben* Reste 3, 9, 27, 20, 60, 58, 52, 34, 41 und 1, unter welchen sich auch die Stammwurzeln 3, 27, 41 und 52 selbst befinden; obwohl in *verschiedener* Ordnung.

Zu II. Für die 10te Stammwurzel $z_1 = 3$ giebt z_1^3 zu p den Rest 27, welches ebenfalls eine der 10ten Stammwurzel $z_2 = 27$ ist; also ist für diesen Fall in (4.) $x = 3$. Nun giebt

$$10. \quad \left\{\begin{array}{llllll} z_1^3 & \dots\dots\dots & & & \text{den Rest } 27 & \text{zu } p, \\ z_1^6 & \dots\dots\dots & & & \text{den Rest } 58 & - \;-, \\ z_1^9 & \dots\dots\dots & & & \text{den Rest } 41 & - \;-, \\ z_1^{12} & \text{oder } z^{1.10+2} & \text{oder } z^2 & & \text{den Rest } \;\;9 & - \;-, \\ z_1^{15} & \text{oder } z^{1.10+5} & \text{oder } z^5 & & - \;\; - \;\; 60 & - \;-, \\ z_1^{18} & \text{oder } z^{1.10+8} & \text{oder } z^8 & & - \;\; - \;\; 34 & - \;-, \\ z_1^{21} & \text{oder } z^{2.10+1} & \text{oder } z^1 & & - \;\; - \;\;\;\; 3 & - \;-, \\ z_1^{24} & \text{oder } z^{2.10+4} & \text{oder } z^4 & & - \;\; - \;\; 20 & - \;-, \\ z_1^{27} & \text{oder } z^{2.10+7} & \text{oder } z^7 & & - \;\; - \;\; 52 & - \;-, \\ z_1^{30} & \text{oder } z^{2.10+10} & \text{oder } z^{10} & & - \;\; - \;\;\;\; 1 & - \;-; \end{array}\right.$$

und *dieselben* Reste zu p geben z_2^1, z_2^2, z_2^3, z_2^4, z_2^5, z_2^6, z_2^7, z_2^8, z_2^9 und z_2^{10}; gemäfs (9.).

Beweis *A.* Für jedes ε in (2.), welches mit δ keinen Theiler > 1 gemein hat, ist nach (§. 60 II.) r_ε eine δte *Stammwurzel* aus 1 zu p. Alle diejenigen x also, welche zu δ *theilerfremd* sind, erfüllen die Gleichung (4.).

B. Nimmt man nun von (4.) die Potenz ε, so ergiebt sich

$$11. \quad z_1^{\varepsilon x} = \mathfrak{G}p + z_2^\varepsilon$$

oder, nach (6.) ausgedrückt,

$$z_1^{n\delta+\varkappa_1} = \mathfrak{G}p + z_2^{\varepsilon} \text{ oder}$$

$$12. \quad z_1^{n\delta} z_1^{\varkappa_1} = \mathfrak{G}p + z_2^{\varepsilon},$$

oder, da aus (1.)

$$13. \quad z_1^{n\delta} = (\mathfrak{G}p + 1)^n = \mathfrak{G}p + 1$$

ist,

$$(\mathfrak{G}p + 1) z_1^{\varkappa_1} = \mathfrak{G}p + z_2^{\varepsilon} \text{ oder}$$

$$14. \quad z_2^{\varepsilon} = \mathfrak{G}p + z_1^{\varkappa_1}.$$

C. Läfst man nun in (6.) ε der Reihe nach alle die Zahlen 1, 2, 3, 4, ... δ durchlaufen, so durchlauft nach (§. 34. I.), da $\varkappa$ und δ nach der Voraussetzung zu einander theilerfremd sind, $\varkappa_1$ in (6.) ebenfalls *alle diese Zahlen,* obwohl in verschiedener Ordnung. Setzt man also in (14.) nach (5. und 6.)

$$15. \quad z_2^{\varepsilon} = \mathfrak{G}p + r_{\varepsilon} \text{ und}$$

$$16. \quad z_1^{\varkappa_1} = \mathfrak{G}p + r_{\varkappa_1}$$

und läfst in (15.) ε alle die Zahlen 1, 2, 3, 4, ... δ durchlaufen, so durchlauft $\varkappa_1$ nach (6.) ebenfalls *alle* diese Zahlen, und folglich durchlauft auch, vermöge (14.), $r_{\varkappa_1}$ in (16.) *alle dieselben* Zahlen wie r_{ε} in (15.), indem nach (14.) z_2^{ε} und $z_1^{\varkappa_1}$ nur um Vielfache von p verschieden sind und sie also *dieselben* Reste r_{ε} und $r_{\varkappa_1}$ zu p geben müssen. Folglich durchlauft r_{ε} in (2.), wenn man der Reihe nach $\varepsilon = 1, 2, 3, 4, \ldots \delta$ setzt, für *jedes* z_2 oder z_1, welches eine δte *Stammwurzel* aus 1 zu p ist, immer *dieselben* Zahlen. Dieses ist was (I.) behauptet.

D. Setzt man (15. und 16.) in (14.), so ergiebt sich

$$\mathfrak{G}p + r_{\varepsilon} = \mathfrak{G}p + \mathfrak{G}p + r_{\varkappa_1}, \text{ oder}$$

$$17. \quad r_{\varepsilon} = \mathfrak{G}p + r_{\varkappa_1}$$

und, da r_{ε} und $r_{\varkappa_1}$ beide $< p$ sind,

$$18. \quad r_{\varepsilon} = r_{\varkappa_1};$$

gemäfs (II. 8.).

E. Anm. Die gegenwärtigen Sätze gehen aus (§. 34. und 40.) hervor.

§. 62.

Lehrsatz.

Wenn in der Zahlengleichung

$$1. \quad x^{\delta} = \mathfrak{G}p + r$$

p *eine Stammzahl,* δ *ein* **Theiler** *von* p — 1 *ist, und* z *ist in*

$$2. \quad z^{\delta} = \mathfrak{G}p + 1$$

irgend eine δ*te* **Stammwurzel** *aus* 1 *zu* p, *und man setzt*

$$3.\quad z^x = \mathfrak{S}p + r_1,$$
$$4.\quad r\,x = \mathfrak{S}p + y \text{ und}$$
$$5.\quad y^\delta = \mathfrak{S}p + \varrho,$$

so ist in (1. *und* 5.)

$$6.\quad r = \varrho$$

für jede δte Stammwurzel z *aus* 1 *zu* p *und für jeden Werth von* $x > 0$ *und* $< \delta + 1$.

Oder in Worten: Die δte Potenz einer beliebigen Zahl x *giebt, wenn δ ein Theiler von* p—1 *ist, zu* p *denselben Rest* r, *wie die δten Potenzen von* xz, xz^2, xz^3, xz^4, ... xz^δ *für jede δte Stammwurzel* z *aus* 1 *zu* p. *Auch giebt die δte Potenz keiner andern Zahlen den Rest* r.

Beispiel. (Aus Taf. I.) Es sei

$$7.\quad x = 12,\quad \delta = 6.$$

Zu $\delta = 6$ ist

$$8.\quad z = 14$$

eine Stammwurzel. Für diese ist in (3.), wenn man x der Reihe nach $= 1$, 2, 3, 4, 5 und 6 setzt,

$$9.\quad r_1 = 14, 13, 60, 47, 48 \text{ und } 1,$$

und in (4.) ist $14.12 = 168 = 2.p + 46$, $13.12 = 156 = 2.p + 34$, $60.12 = 720 = 8.p + 49$, $47.12 = 564 = 9.p + 15$, $48.12 = 576 = 9.p + 27$ und $1.12 = 0.p + 12$, also

$$10.\quad y = 46, 34, 49, 15, 27 \text{ und } 12.$$

Endlich ist für (5.), wie es sich aus der Tafel entnehmen läfst, wenn man 46, 34, 49, 15, 27 und 12 in der *obersten* horizontalen Reihe aufsucht und die zugehörigen Zahlen in der *sechsten* horizontalen Zeile nimmt,

$$11.\quad 46^6 = \mathfrak{S}p + 34,\ 34^6 = \mathfrak{S}p + 34,\ 49^6 = \mathfrak{S}p + 34,\ 15^6 = \mathfrak{S}p + 34,$$
$$27^6 = \mathfrak{S}p + 34 \text{ und } 12^6 = \mathfrak{S}p + 34.$$

Also sind für (5.) alle $\varrho = 34$ und $= r$.

Beweis. *A*. In (1.) x mit z^x multiplicirt, giebt $(xz^x)^\delta = x^\delta z^{x\delta}$. Aber $z^\delta = \mathfrak{S}p + 1$ (2.), also $z^{x\delta} = (\mathfrak{S}p + 1)^x = \mathfrak{S}p + 1$ und folglich

$$12.\quad (xz^x)^\delta = (\mathfrak{S}p + 1)x^\delta = \mathfrak{S}p + x^\delta = \mathfrak{S}p + \mathfrak{S}p + r\ (1.) = \mathfrak{S}p + r;$$

also giebt x, multiplicirt mit *jeder* Potenz z^x von z, die δte Potenz *derselben* Reste r, wie die δte Potenz von x selbst.

B. Zu jedem *Theiler* δ von $p-1$ gehören zu *demselben* r *nur* δ verschiedene Werthe von x (§. 54. I.). Die Multiplication von x mit z^1, z^2,

$z^3, \ldots z^\delta$ giebt δ Zahlen, die, zur Potenz δ erhoben, *denselben* Rest r lassen, und alle diese Zahlen sind *verschieden:* denn zu $z^1, z^2, z^3, \ldots z^\delta$ sind in (3.), da z die δte *Stammwurzel* aus 1 zu p sein soll, alle die Reste r_1 *verschieden,* also auch alle die y in (4.), und alle die ϱ in (5.); mithin giebt die Multiplication von x mit $z^1, z^2, z^3, \ldots z^\delta$ *alle* die δ Zahlen, von welchen die Potenz δ zu p *denselben* Rest r läfst; und es giebt keinen andern.

Dies zusammen ist, was der Lehrsatz in *Worten* behauptet.

C. Dafs das, was der Lehrsatz in *Zeichen* ausspricht, das Nemliche ist, ergiebt sich wie folgt. Es ist

$$13.\quad (xz^x)^\delta = (x(\mathfrak{S}p+r_1))^\delta\,(3.) = \mathfrak{S}p+(r_1x)^\delta = \mathfrak{S}p+(\mathfrak{S}p+y)^\delta\,(4.) = \mathfrak{S}p+y^\delta = \mathfrak{S}p+\varrho\,(5.).$$

Aber

$$14.\quad x^\delta = \mathfrak{S}p+r,$$

und da $(xz^x)^\delta$ und x^δ, wie sich fand, zu p *gleiche* Reste lassen, so ist

$$15.\quad r = \varrho;$$

gemäfs (6.).

Anm. *D.* Der Satz beruht insbesondere auf (§. 54.).

§. 63.

Lehrsatz.

I. *Die Anzahl der Stammwurzeln* z_δ *aus* 1 *zu einer Stammzahl* p, *für jeden beliebigen Exponenten* δ, *der nach* (§. 58.) *in* $p-1$ *aufgehen mufs, also auch für den Exponenten* $p-1$ *selbst, ist der Anzahl der Zahlen* >0 *und* $<\delta$ *gleich, die mit* δ *keinen Theiler* >1 *gemein haben.*

II. *Zu jedem andern in* $p-1$ *aufgehenden Exponenten gehören andere Stammwurzeln aus* 1 *zu* p.

III. *Die Stammwurzeln* z_δ *aus* 1 *zu* p, *mit allen den verschiedenen Theilern* δ *von* $p-1$, *also auch mit* $p-1$ *selbst zu Exponenten, sind zusammen alle die Zahlen* $1, 2, 3, 4, \ldots p-1$.

IV. *Wenn man eine der Hauptstammwurzeln* z_{p-1} *kennt, so geben die Reste ihrer verschiedenen Potenzen zu* p, *von der* 1*ten an, bis zur* $p-1$*ten, nicht allein die übrigen Hauptstammwurzeln, sondern auch die sämmtlichen Stammwurzeln für alle in* $p-1$ *aufgehende Exponenten. Die Hauptstammwurzeln* z_{p-1} *aus* 1 *zu* p *sind, wenn* z_{p-1} *eine derselben ist, in*

$$1.\quad z_{p-1}^x = \mathfrak{S}p+r_x$$

diejenigen r_x, *deren Zeiger* x *mit* $p-1$ *keinen Theiler* >1 *gemein haben. Die Stammwurzeln* z_δ *dagegen aus* 1 *zu* p, *für einen beliebigen in* $p-1$ *aufgehenden Exponenten* δ, *sind die* r_x, *deren Zeiger* x *mit* $p-1$ *zum gröfsten Gemeintheiler* $\frac{p-1}{\delta}$ *haben; so dafs man also vermittels einer der Hauptstammwurzeln alle Stamm- und Hauptstammwurzeln unmittelbar unter den Potenzenresten jener einen Hauptstammwurzel findet.*

Beispiele. (Aus Taf. I.) Was der Lehrsatz behauptet, wird sich zusammengenommen in dem Beispiel $p=61$ in folgender Übersicht zeigen.

2. Es sind die *Hauptstammwurzeln*
$z_{p-1} =$ 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55 und 59,
z. B. für $z_{p-1}=2$ in (1.) die Reste r_x für
$x=$ 1, 7, 49, 23, 47, 13, 41, 29, 59, 11, 43, 17, 53, 19, 37 und 31;
für $z_{p-1}=6$ in (1.) die Reste r_x für
$x=$ 43, 1, 7, 29, 41, 19, 23, 47, 17, 53, 49, 11, 59, 37, 31 und 13;
für $z_{p-1}=7$ in (1.) die Reste r_x für
$x=$ 49, 43, 1, 47, 23, 37, 29, 41, 11, 59, 7, 53, 17, 31, 13 und 19.
. . . .

3. Es sind die $\delta=30$ten Stammwurzeln $z_{30} =$ 4, 5, 19, 36, 39, 45, 46, 49,
z. B. für $z_{p-1}=2$ in (1.) die Reste r_x für $x=$ 2, 22, 26, 14, 46, 34, 58, 38;
für $z_{p-1}=6$ - - - - r_x - $x=$ 26, 46, 38, 2, 58, 22, 34, 14;
für $z_{p-1}=7$ - - - - r_x - $x=$ 38, 58, 14, 26, 34, 46, 22, 2.
. . . .

4. Es sind die $\delta=20$ten Stammwurzeln $z_{20} =$ 8, 23, 24, 28, 33, 37, 38, 53,
z. B. für $z_{p-1}=2$ in (1.) die Reste r_x für $x=$ 3, 57, 9, 51, 21, 39, 27, 33;
für $z_{p-1}=6$ - - - - r_x - $x=$ 9, 51, 27, 33, 3, 57, 21, 39;
für $z_{p-1}=7$ - - - - r_x - $x=$ 27, 33, 21, 39, 9, 51, 3, 57.
. . . .

5. Es sind die $\delta=15$ten Stammwurzeln $z_{15} =$ 12, 15, 16, 22, 25, 42, 56, 57,
z. B. für $z_{p-1}=2$ in (1.) die Reste r_x für $x=$ 8, 28, 4, 16, 44, 56, 52, 32;
für $z_{p-1}=6$ - - - - r_x - $x=$ 44, 4, 52, 28, 32, 8, 16, 56;
für $z_{p-1}=7$ - - - - r_x - $x=$ 32, 52, 16, 4, 56, 44, 28, 8.
. . . .

6. Es sind die $\delta = 12$ten Stammwurzeln $z_{12} = 21, 29, 32, 40,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste r_x für $x = 55, 35, 5, 25;$
für $z_{p-1} = 6$ - - - - r_x - $x = 25, 5, 35, 55;$
für $z_{p-1} = 7$ - - - - r_x - $x = 55, 35, 5, 25.$
. . . .

7. Es sind die $\delta = 10$ten Stammwurzeln $z_{10} = 3, 27, 41, 52,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste r_x für $x = 6, 18, 54, 42;$
für $z_{p-1} = 6$ - - - - r_x - $x = 18, 54, 42, 6;$
für $z_{p-1} = 7$ - - - - r_x - $x = 54, 42, 6, 18.$
. . . .

8. Es sind die $\delta = 6$ten Stammwurzeln $z_6 = 14, 48,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste r_x für $x = 50, 10;$
für $z_{p-1} = 6$ - - - - r_x - $x = 50, 10;$
für $z_{p-1} = 7$ - - - - r_x - $x = 50, 10.$
. . . .

9. Es sind die $\delta = 5$ten Stammwurzeln $z_5 = 9, 20, 34, 58,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste r_x für $x = 12, 24, 48, 36;$
für $z_{p-1} = 6$ - - - - r_x - $x = 36, 12, 24, 48;$
für $z_{p-1} = 7$ - - - - r_x - $x = 48, 36, 12, 24.$
. . . .

10. Es sind die $\delta = 4$ten Stammwurzeln $z_4 = 11, 50,$
z. B. für $z_{p-1} = 2$ in (1.) die Reste r_x für $x = 15, 45;$
für $z_{p-1} = 6$ - - - - r_x - $x = 45, 15;$
für $z_{p-1} = 7$ - - - - r_x - $x = 15, 45.$
. . . .

11. Es sind die $\delta = 3$ten Stammwurzeln $z_3 = 13, 47;$
z. B. für $z_{p-1} = 2$ in (1.) die Reste r_x für $x = 40, 20;$
für $z_{p-1} = 6$ - - - - r_x - $x = 40, 20;$
für $z_{p-1} = 7$ - - - - r_x - $x = 40, 20.$
. . . .

12. Es ist die $\delta = 2$te Stammwurzel $z_2 = 60,$
z. B. für $z_{p-1} = 2$ in (1.) der Rest r_x für $x = 30;$
für $z_{p-1} = 6$ - - - - r_x - $x = 30;$
für $z_{p-1} = 7$ - - - - r_x - $x = 30.$
. . . .

13. $\Big\{$ Es ist die $\delta = 1$te Stammwurzel $z_1 = 1$ für alle z_{p-1} in (1.) der Rest r_x für $x = 60$.

Hier sind nun, wie man sieht,

a. In (2.) die Werthe von x für die verschiedenen *Hauptstammwurzeln* z_{p-1} *dieselben;* wie es sein mufs, da *jede* Hauptstammwurzel das *Nemliche* giebt.

b. In (2.), für die Hauptstammwurzeln $z_{p-1} = z_{60}$, sind die Werthe 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53 und 59 von x alle die Zahlen, welche mit $p-1 = 60$ keinen Theiler > 1 gemein haben.

In (3.), für die Stammwurzeln $z_\delta = z_{30}$, sind die Werthe 2, 14, 22, 26, 34, 38, 46 und 58 von x alle die Zahlen, welche mit $p-1 = 60$, $\frac{p-1}{\delta} = \frac{60}{30} = 2$ zum *gröfsten Gemeintheiler* haben.

In (4.), für die Stammwurzeln $z_\delta = z_{20}$, sind die Werthe 3, 9, 21, 27, 33, 39, 51 und 57 von x alle die Zahlen, welche mit $p-1 = 60$, $\frac{p-1}{\delta} = \frac{60}{20} = 3$ zum *gröfsten Gemeintheiler* haben.

Und so weiter in (5. 6. 7. .... 13.) für $\delta = 15, 12, 10, 6, 5, 4, 3, 2$ und 1; wie es gemäfs (IV.) sein soll.

c. Die *Anzahl* der verschiedenen Stammwurzeln ist jedesmal der Anzahl der Zahlen gleich, welche mit δ keinen Theiler > 1 gemein haben; gemäfs (I.). Nemlich:

Zu $\delta = p-1 = 60$ giebt es gemäfs (2.) 16 Stammwurzeln,
und die 16 Zahlen 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53 und 59 haben mit $\delta = 60$ keinen Theiler > 1 gemein.

Zu $\delta = 30$ giebt es gemäfs (3.) 8 Stammwurzeln,
und die 8 Zahlen 1, 7, 11, 13, 17, 19, 23 und 29 haben mit $\delta = 30$ keinen Theiler > 1 gemein.

Für $\delta = 20$ giebt es gemäfs (3.) 8 Stammwurzeln,
und die 8 Zahlen 1. 3, 7, 9, 11, 13, 17 und 19 haben mit $\delta = 20$ keinen Theiler > 1 gemein.

Und so weiter.

d. Zu jedem Exponenten δ gehören, wie (2. 3. .... 13.) zeigen, *andere* Stammwurzeln z_δ; gemäfs (II.).

e. Alle Stammwurzeln in (2. 3. .... 13.) sind zusammen *alle* die Zahlen 1, 2, 3, 4, ... 60; gemäfs (III.).

Beweis. *A.* Der Beweis von (IV.) liegt unmittelbar in (§. 60. I. und II.) und ist daselbst ausgesprochen.

B. Nach (§. 60. I.) sind in

$$14. \quad x_\delta^n = \mathfrak{S}p + r_n$$

diejenigen r_n, für welche der *gröfste Gemeintheiler* von x und δ, λ ist, *alle* die $\frac{\delta}{\lambda} = \delta_1$ten Stammwurzeln aus 1 zu p.

a. Setzt man

$$15. \quad x = 1, 2, 3, 4, \ldots \delta,$$

so haben von diesen δ Zahlen

$$16. \quad \text{die } \frac{\delta}{\lambda} = \delta_1 \text{ Zahlen } \lambda, 2\lambda, 3\lambda, 4\lambda, \ldots \frac{\lambda}{\delta}.\lambda,$$

und *keine andern*, mit δ den Theiler λ gemein. Nur diese $\frac{\delta}{\lambda} = \delta_1$ Zahlen unter denen (15.) kommen für die Werthe von x, welche in (14.) durch die r die $\frac{\delta}{\lambda} = \delta_1$ten Stammwurzeln geben, in Betracht; denn alle diese x *sollen* mit λ *aufgehen*. Aber *unter* den δ_1 Zahlen (16.) befinden sich auch *alle* x, auf welche es ankommt.

b. Es sollen aber von den δ_1 Zahlen (16.), *unter welchen* sich die gesuchten x befinden, nur *diejenigen* genommen werden, welche mit

$$17. \quad \delta = \delta_1\lambda \ (16.)$$

keinen gröfsern Theiler als λ gemein haben. Diese sind die *gesuchten* x. Drückt man die δ_1 Zahlen (16.) allgemein durch

$$18. \quad \varepsilon = \tau\lambda$$

aus, wo nun $\tau = 1, 2, 3, 4, \ldots \delta_1 \left(= \frac{\delta}{\lambda}\right)$ ist, so sind jene *gesuchten* x, welche mit δ *keinen gröfsern* Theiler als x gemein haben, offenbar diejenigen, und nur diejenigen ε, für welche τ in (18.) mit δ_1 in (17.) *keinen Theiler* > 1 gemein hat: denn so wie τ noch irgend einen Theiler $\mu > 1$ von δ mit δ_1 gemein hat, so ist der *gröfste* Gemeintheiler von ε und δ nicht mehr λ, sondern $\mu\lambda > \lambda$.

c. Es folgt also, dafs die *Anzahl* derjenigen x, deren *gröfster Gemeintheiler* mit δ, λ ist, *dieselbe* sein mufs, wie die Anzahl der Zahlen, welche mit $\delta_1 = \frac{\delta}{\lambda}$ *keinen Theiler* > 1 gemein haben, oder welche zu δ_1 *theilerfremd* sind.

d. Diese x nun geben *alle* die $\delta_1 = \frac{\delta}{\lambda}$ten Stammwurzeln: also ist die *Anzahl* dieser $\frac{\delta}{\lambda}$ten Stammwurzeln der Anzahl der zu $\delta_1 = \frac{\delta}{\lambda}$ *theilerfremden* Zahlen gleich. Folglich ist allgemein, δ statt δ_1 gesetzt, die Anzahl der Stammwurzeln aus 1 zu p für einen beliebigen Exponenten δ, welcher in $p-1$ *aufgeht*, der Anzahl der Zahlen >0 und $<\delta$ gleich, die mit δ keinen Theiler >1 gemein haben; gemäfs (I.).

C. Gehörte eine und dieselbe Stammwurzel z zu zwei verschiedenen in $p-1$ aufgehenden Exponenten δ_1 und δ_2, so müfste

$$19. \quad z^{\delta_1} = \mathfrak{G}p + 1 \text{ und zugleich}$$

$$20. \quad z^{\delta_2} = \mathfrak{G}p + 1$$

sein. Dies ist nicht der Fall; denn wenn z. B. von den beiden Exponenten δ_1 und δ_2 der letztere der *gröfsere* ist, so giebt nicht z^{δ_1} den Rest 1 zu p, sondern einen Rest >1, indem *alle* Potenzen $z^1, z^2, z^3, \ldots z^{\delta_2}$, und also auch z^{δ_1} *andere* Reste als 1 geben und *zuerst* die Potenz z^{δ_2} den Rest 1 giebt. So will es die Bedingung, dafs z eine $\delta_2$te *Stammwurzel* sei. Also gehören zu jedem in $p-1$ aufgehenden Exponenten δ *andere* Stammwurzeln aus 1 zu p; gemäfs (II.).

D. Jede der Zahlen $1, 2, 3, 4, \ldots p-1$ giebt, zu irgend einer Potenz erhoben, deren Exponent δ entweder $p-1$ selbst, oder ein *Theiler* von $p-1$ ist, nachdem $z^1, z^2, z^3, \ldots z^{\delta-1}$ andere Reste gegeben haben, zu z^δ den Rest 1 (§. 58.). *Jede* der Zahlen $1, 2, 3, \ldots p-1$ ist also nothwendig irgend eine *Stammwurzel*. Ihre Potenzen erreichen immer, entweder schon mit irgend einem Theiler δ von $p-1$, oder mit $p-1$ selbst zum Exponenten, *jedenfalls* den Rest 1. Aber zu jedem Exponenten δ gehören *andere* Stammwurzeln (II.): also kommt jede der Zahlen als Stammwurzel *nur einmal* vor; *alle* aber kommen als solche vor. Also sind die verschiedenen möglichen Stammwurzeln alle die Zahlen $1, 2, 3, 4, \ldots p-1$; gemäfs (III.).

Anm. *E.* Die gegenwärtigen Sätze gehen aus (§. 58. und 60.) hervor, mit Hülfe der Erwägungen in (*B.*).

§. 64.

Lehrsatz.

I. *Wenn* p *eine Stammzahl ist,* δ *und* μ *beliebige Zahlen sind, und man setzt in*

$$1. \quad z^\delta = \mathfrak{G}p + r \text{ und}$$

$$2. \quad z^{\mu\delta} = \mathfrak{G}p + \varrho$$

der Reihe nach

$$3. \quad z = 1, 2, 3, 4, \ldots\ldots p-1,$$

so sind alle die Werthe von ϱ *in* (2.) *unter den Werthen von* r *in* (1.) *mitbegriffen.*

II. *Wenn* $\lambda_1, \lambda_2, \lambda_3, \ldots\ldots$ *die in* p — 1 *aufgehenden Stammzahlen sind, und* $\delta\lambda_1, \delta\lambda_2, \delta\lambda_3, \ldots\ldots$ *gehen ebenfalls noch in* p — 1 *auf, also auch* δ, *so erhält man, wenn man von den Werthen, welche* r *in* (1.) *für* z = 1, 2, 3, 4, ... p — 1 *bekommt, die Werthe ausschliefst, welche in*

$$4. \quad z^{\delta\lambda_1} = \mathfrak{G}p + \varrho_1, \quad z^{\delta\lambda_2} = \mathfrak{G}p + \varrho_2, \quad z^{\delta\lambda_3} = \mathfrak{G}p + \varrho_3, \quad \ldots\ldots$$

die Reste $\varrho_1, \varrho_2, \varrho_3, \ldots\ldots$, *ebenfalls für* z = 1, 2, 3, 4, ... p — 1 *annehmen und welche nach* (I.) *unter den Werthen von* r *in* (1.) *mitbegriffen sind, die* $\frac{p-1}{\delta}$*ten Stammwurzeln aus* 1 *zu* p.

III. *Für* $\delta = 1$ *erhält man also die Hauptstammwurzeln, wenn man von den Zahlen* 1, 2, 3, 4, ... p — 1 *selbst die Reste zu denjenigen ihrer Potenzen ausschliefst, deren Exponenten* $\lambda_1, \lambda_2, \lambda_3, \ldots\ldots$ *die in* p — 1 *aufgehenden Stammzahlen sind.*

IV. *Auch erhält man die* $\frac{p-1}{\delta}$*ten Stammwurzeln aus* 1 *zu* p, *wenn man von den Werthen von* r *in* (1.) *diejenigen ausschliefst, für welche, wenn* x *die sämmtlichen Theiler von* $\frac{p-1}{\delta}$ *bezeichnet, in*

$$5. \quad r^x = \mathfrak{G}p + R,$$

R = 1 *ist.*

Anm. Will man die $\frac{p-1}{\delta}$ten Stammwurzeln *nach* (II.) berechnen, so mufs man zunächst alle r in (1.) suchen. Sie ergeben sich schon, wenn man $z = 1, 2, 3, 4, \ldots\ldots \frac{1}{2}(p-1)$ setzt; denn für die *übrigen* z sind nach (§. 54. V.) die r entweder *dieselben*, zu $p-z$, oder sie ergeben sich aus jenen, wenn man sie von p *abzieht*. In (4.) sind dann ebenfalls den z alle die Werthe $1, 2, 3, 4, \ldots\ldots \frac{1}{2}(p-1)$ beizulegen, aber *nur* für die Exponenten $\delta\lambda_1, \delta\lambda_2, \delta\lambda_3, \ldots\ldots$

Will man dagegen die $\frac{p-1}{\delta}$ten Stammwurzeln *nach* (IV.) berechnen, so sind, nachdem, wie vorhin, die r in (1.) gefunden worden sind, den r in (5.) *nur alle die gefundenen Werthe von* r beizulegen nöthig: aber für *alle* die verschiedenen Exponenten x, welche in $\frac{p-1}{\delta}$ aufgehen.

Beispiele. (Aus Taf. I.) Zu I. In (1. und 2.) ist, der Tafel gemäfs, z. B.

$$6.\quad \left\{ \begin{array}{lll} \text{Für } & \delta = 6, & r = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60, \\ - & \mu\delta = 12, & \varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots, \\ - & \mu\delta = 18, & \varrho = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60, \\ - & \mu\delta = 24, & \varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots, \\ - & \mu\delta = 30, & \varrho = 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 60, \\ - & \mu\delta = 36, & \varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots, \\ - & \mu\delta = 42, & \varrho = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60, \\ - & \mu\delta = 48, & \varrho = 1 \ldots 9\ 20 \ldots 34 \ldots \ldots 58 \ldots, \\ - & \mu\delta = 54, & \varrho = 1\ 3\ 9\ 20\ 27\ 34\ 41\ 52\ 58\ 60. \end{array} \right.$$

Immer sind die ϱ in (2.), wie man sieht, unter den r *mitbegriffen*.

Ist δ zu $p-1$ *theilerfremd*, so sind nach (§. 55. II.) die r in (1.) alle die Zahlen $1, 2, 3, 4, \ldots. p-1$; also sind auch dann in (2.) die ϱ unter den r in (1.) *mitbegriffen*; gemäfs (I.).

Zu II. Die in $p-1=60$ aufgehenden *Stammzahlen* $\lambda_1, \lambda_2, \lambda_3, \ldots.$ sind 2, 3 und 5. $\delta=4$ ist einer der Theiler von $p-1$, und von den Exponenten $\delta\lambda_1=8$, $\delta\lambda_2=12$ und $\delta\lambda_3=20$, für (4.), gehen $\delta\lambda_2=12$ und $\delta\lambda_3=20$ in $p-1$ auf. Nun ist in (1. und. 4.) nach der Tafel:

$$7.\quad \left\{ \begin{array}{lll} \text{Für } & \delta = 4, & r = 1\ 9\ 12\ 13\ 15\ 16\ 20\ 22\ 25\ 34\ 42\ 47\ 56\ 57\ 58, \\ - & \delta\lambda_2 = 12, & \varrho_2 = 1\ 9 \ldots\ldots\ldots\ldots 20 \ldots\ldots 34 \ldots\ldots\ldots\ldots 58, \\ - & \delta\lambda_3 = 20, & \varrho_3 = 1 \ldots\ldots 13 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 47 \ldots\ldots\ldots. \end{array} \right.$$

Schliefst man die ϱ_2 und ϱ_3 von den r aus, so bleiben 12, 15, 16, 22, 25, 42, 56 und 57 übrig, und diese Zahlen sind, wie die Tafel zeigt, die $\frac{p-1}{\delta} = \frac{60}{4} = 15$ten *Stammwurzeln* aus 1 zu p; gemäfs (II.).

Zu III. Für die *Stammzahlen* $\lambda_1=2$, $\lambda_2=3$ und $\lambda_3=5$, welche in $p-1=60$ aufgehen, und für $\delta=1$, ist in (4.), der Tafel zufolge:

$$8.\quad \left\{ \begin{array}{l} \text{Für } \lambda_1=2,\ \varrho_1 = 1\,3\,4\,5 .. 9 \ldots 12\,13\,14\,15\,16\,19\,20 \ldots 22 \ldots \ldots 25\,27 \ldots \ldots \ldots \ldots 34\,36 \ldots \ldots 39 \ldots 41\,42\,45\,46\,47\,48\,49 \ldots 52 \ldots 56\,57\,58\,60, \\ \text{Für } \lambda_2=3,\ \varrho_2 = 1\,3 \ldots 8\,9\,11 \ldots \ldots \ldots \ldots \ldots \ldots 20 \ldots \ldots 23\,24 \ldots 27\,28 \ldots \ldots 33\,34 \ldots 37\,38 \ldots \ldots 41 \ldots \ldots \ldots \ldots \ldots \ldots 50\,52\,53 \ldots \ldots 58\,60, \\ \text{Für } \lambda_3=5,\ \varrho_3 = 1 \ldots\ldots\ldots 11 \ldots 13\,14 \ldots \ldots \ldots \ldots 21 \ldots \ldots \ldots \ldots \ldots \ldots 29\,32 \ldots \ldots \ldots \ldots \ldots \ldots 40 \ldots \ldots \ldots \ldots 47\,48 \ldots 50 \ldots \ldots \ldots \ldots \ldots 60. \end{array} \right.$$

Schliefst man diese verschiedenen Zahlen $\varrho_1, \varrho_2, \varrho_3$ von den Zahlen 1, 2, 3, 4, ... 60 aus, so bleiben die Zahlen 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55 und 59 übrig, und diese sind die *Hauptstammwurzeln* aus 1 zu p; gemäfs (III.).

Zu IV. Für $\delta=5$ z. B. ist $\frac{p-1}{\delta} = \frac{60}{5} = 12$. Die Theiler von 12 sind 2, 3, 4 und 6, also ist in (5.) $x = 2, 3, 4$ und 6. Nun ist für (1. u. 5.) nach der Tafel:

9.

Für $\delta=5$,	$r=$	1	11	13	14	21	29	32	40	47	48	50	60;
Für $x=2$,	$R=$	1	60	47	13	14	56	48	14	13	47	60	1,
- $x=3$,	$R=$	1	50	1	60	50	27	11	11	1	60	11	60,
- $x=4$,	$R=$	1	1	13	47	10	25	47	13	47	13	1	1,
- $x=6$,	$R=$	1	60	1	1	60	48	60	60	1	1	60	1.

Die Werthe 1, 11, 13, 14, 47, 48 und 60 geben für ein oder das andere x in (5.) den Rest $R=1$. Sie müssen also von den Werthen von r in der obersten Zeile (9.) ausgeschlossen werden. Die übrig bleibenden r sind 21, 29, 32 und 40, und diese sind, wie die Tafel zeigt, die $\frac{p-1}{\delta}=12$ten Stammwurzeln aus 1 zu p; gemäfs (IV.).

Beweis. Von I. *A.* Setzt man, für irgend ein bestimmtes r,

$$10.\quad r^{\mu} = \mathfrak{S}p + k,$$

so ist jedenfalls k *irgend eine* der Zahlen $x = 1, 2, 3, 4, \ldots\ldots p-1$. Nun giebt die δte Potenz von (10.)

$$11.\quad r^{\mu\delta} = \mathfrak{S}p + k^{\delta}.$$

Aber da die δten Potenzen *aller* der Zahlen 1, 2, 3, ... $p-1$ in (1.) nur die Reste r geben, so kann auch die δte Potenz von k nur *eins der r* geben, z. B. r_1; folglich ist

$$12.\quad k^{\delta} = \mathfrak{S}p + r_1,$$

mithin in (11.)

$$13.\quad r^{\mu\delta} = \mathfrak{S}p + \mathfrak{S}p + r_1 = \mathfrak{S}p + r_1.$$

Zufolge (2.) ist aber

$$14.\quad r^{\mu\delta} = \mathfrak{S}p + \varrho,$$

also ist aus (13. und 14.) $\mathfrak{S}p + r_1 = \mathfrak{S}p + \varrho$ oder

$$15.\quad \varrho = \mathfrak{S}p + r_1$$

und, da r_1 und ϱ beide $<p$ sind,

$$16.\quad \varrho = r_1;$$

mithin ist ϱ irgend einem r gleich, und folglich sind *alle* Werthe von ϱ in (1.) *mitbegriffen.*

Beweis von II. *B.* Für *alle r* in (1.) ist

$$17.\quad r^{\frac{p-1}{\delta}} = \mathfrak{S}p + 1,$$

denn die $\frac{p-1}{\delta}$te Potenz von (1.) giebt

$$18\quad z^{\delta.\frac{p-1}{\delta}} = z^{p-1} = \mathfrak{S}p + r^{\frac{p-1}{\delta}}$$

und. da nach dem Fermatschen Lehrsatz (§. 40.) $z^{p-1} = \mathfrak{G}p+1$ ist, für *jedes z:*

$$19. \quad \mathfrak{G}p + r^{\frac{p-1}{\delta}} = \mathfrak{G}p+1;$$

woraus (17.) folgt.

C. Nun ist es eine Bedingung für die $\frac{p-1}{\delta}$ten *Stammwurzeln z*, dafs

$$20. \quad z^{\frac{p-1}{\delta}} = \mathfrak{G}p+1$$

sei: also *kann jedes r* in (17.) eine $\frac{p-1}{\delta}$te Stammwurzel sein. Und zwar eignen sich *keine andern* Zahlen z als die r zu $\frac{p-1}{\delta}$ten Stammwurzeln; denn *jede* Stammwurzel z mufs $z^{\frac{p-1}{\delta}} = \mathfrak{G}p+1$ geben, und giebt sie den Rest 1, so ist sie auch nach (17.) ein r; denn *alle r* geben diesen Rest.

D. Aber *nicht alle* die r in (17.) sind $\frac{p-1}{\delta}$te Stammwurzeln aus 1 zu p, weil schon *niedrigere* Potenzen als die $\frac{p-1}{\delta}$ten von r den Rest 1 zu p lassen können; und zwar sind alle diejenigen, und *nur* diejenigen r, welche mit Exponenten, die in $\frac{p-1}{\delta}$ *aufgehen,* schon den Rest 1 zu p lassen, *nicht* $\frac{p-1}{\delta}$te Stammwurzeln. Denn gesetzt es sei

$$21. \quad \frac{p-1}{\delta} = \varkappa\sigma,$$

so dafs $\varkappa$ in $\frac{p-1}{\delta}$ aufgeht, so ist, wenn schon

$$22. \quad r^{\varkappa} = \mathfrak{G}p+1$$

giebt, r *nicht* eine $\frac{p-1}{\delta}$te, sondern *kann* schon eine $\varkappa$te Stammwurzel sein, oder selbst eine Stammwurzel für einen *noch niedrigern,* in $\varkappa$ aufgehenden Exponenten. Hingegen kann, wenn z eine $\varkappa$te Stammwurzel, also

$$23. \quad z^{\varkappa} = \mathfrak{G}p+1$$

ist und $\varkappa$ *nicht* in $\frac{p-1}{\delta}$ aufgeht, also etwa

$$24. \quad \frac{p-1}{\delta} = \varkappa\sigma + \varrho$$

ist, wo $\varrho < \varkappa$, dieses z keines der r in (17.) sein. Denn da z eine $\varkappa$te Stammwurzel sein soll, so geben alle die Potenzen z^1, z^2, z^3, ... $z^{\varkappa-1}$, also auch z^{ϱ}, *nicht den Rest* 1. Aus (23.) und (24.) aber ist

$$25. \quad z^{\frac{p-1}{\delta}} = z^{\varkappa\sigma+\varrho} = z^{\varkappa\sigma} z^{\varrho} = (\mathfrak{G}p+1)^{\sigma} z^{\varrho} = \mathfrak{G}p + z^{\varrho},$$

und z^{ϱ} ist *nicht* $=\mathfrak{S}p+1$: also ist auch $z^{\frac{p-1}{\delta}}$ in (25.) *nicht* $=\mathfrak{S}p+1$; wie es für *alle* r in (17.) sein mufs; so dafs also z *keins* der r in (17.) sein kann.

Also alle r, welche schon mit Exponenten, die in $\frac{p-1}{\delta}$ *aufgehen*, und nur mit *solchen* Exponenten, den Rest 1 zu p lassen, sind *nicht* $\frac{p-1}{\delta}$te Stammwurzeln, und man mufs sie folglich von den r, die der Gleichung (17.) genugthun, *ausschliefsen*.

E. Es ist aber nur nöthig, diejenigen r auszuschliefsen, welche mit dem *höchsten* in $\frac{p-1}{\delta}$ *aufgehenden* Exponenten schon den Rest 1 zu p lassen; denn wenn ein *niedrigerer* in $\frac{p-1}{\delta}$ aufgehender Exponent x schon

$$26.\quad r^{x}=\mathfrak{S}p+1$$

giebt, so ist auch für *das selbe* r:

$$27.\quad r^{2x},\ r^{3x},\ \ldots\ \text{bis zu}\ r^{\frac{p-1}{\delta}}=\mathfrak{S}p+1.$$

F. Die *höchsten* in $\frac{p-1}{\delta}$ aufgehenden Exponenten sind aber offenbar $\frac{p-1}{\delta\lambda_1}$, $\frac{p-1}{\delta\lambda_2}$, $\frac{p-1}{\delta\lambda_3}$ etc.; denn die Quotienten von $\frac{p-1}{\delta}$ durch selbige sind

$$28.\quad \frac{p-1}{\delta}:\frac{p-1}{\delta\lambda_1}=\lambda_1,\quad \frac{p-1}{\delta}:\frac{p-1}{\delta\lambda_2}=\lambda_2,\quad \frac{p-1}{\delta}:\frac{p-1}{\delta\lambda_3}=\lambda_3,\ \ldots,$$

und diese Quotienten $\lambda_1, \lambda_2, \lambda_3, \ldots$ sind *Stammzahlen*, und folglich nicht weiter theilbar.

G. Diejenigen r nun, welche

$$29.\quad r^{\frac{p-1}{\delta\lambda_1}}=\mathfrak{S}p+1,\quad r^{\frac{p-1}{\delta\lambda_2}}=\mathfrak{S}p+1,\quad r^{\frac{p-1}{\delta\lambda_3}}=\mathfrak{S}p+1,\ \ldots$$

geben, sind die ϱ in (4.), die zufolge (I.), wenn man nemlich in (2.) λ_1, λ_2, λ_3, ... statt μ setzt, unter den Werthen von r in (1.) mitbegriffen sind. Denn es giebt (4.), wenn man darin die $\frac{p-1}{\delta\lambda_1}$, $\frac{p-1}{\delta\lambda_2}$, $\frac{p-1}{\delta\lambda_3}$, ...ten Potenzen nimmt,

$$30.\quad \begin{cases} z^{\frac{p-1}{\delta\lambda_1}\cdot\delta\lambda_1}=z^{p-1}=\mathfrak{S}p+r^{\frac{p-1}{\delta\lambda_1}},\\ z^{\frac{p-1}{\delta\lambda_2}\cdot\delta\lambda_2}=z^{p-1}=\mathfrak{S}p+r^{\frac{p-1}{\delta\lambda_2}},\\ z^{\frac{p-1}{\delta\lambda_3}\cdot\delta\lambda_3}=z^{p-1}=\mathfrak{S}p+r^{\frac{p-1}{\delta\lambda_3}},\\ \ldots\ldots\ldots\ldots\ldots \end{cases}$$

woraus, da nach dem Fermatschen Lehrsatz (§. 40.) $x^{p-1}=\mathfrak{S}p+1$ ist,

$$31.\quad \varrho^{\frac{p-1}{\delta\lambda_1}}=\mathfrak{S}p+1,\quad \varrho^{\frac{p-1}{\delta\lambda_2}}=\mathfrak{S}p+1,\quad \varrho^{\frac{p-1}{\delta\lambda_3}}=\mathfrak{S}p+1,\quad \ldots\ldots$$

folgt.

Man darf also nur die Werthe der ϱ in (4.) von den Werthen der r in (1.) *ausschliefsen*, so erhält man die $\frac{p-1}{\delta}$ten *Stammwurzeln* aus 1 zu p. Dieses ist was (II.) behauptet.

Beweis von III. *H.* Was (III.) aussagt, folgt unmittelbar aus (II.) für den besondern Fall $\delta=1$: denn in diesem Fall sind die r in (1.) alle die Zahlen 1, 2, 3, 4, ... $p-1$ selbst.

Beweis von IV. *I.* Wie in (*D.*) bewiesen, sind diejenigen r in (1.), von welchen schon Potenzen mit Exponenten x, die in $\frac{p-1}{\delta}$ *aufgehen*, und *nur* mit *solchen* Exponenten,

$$32.\quad r^x=\mathfrak{S}p+1$$

geben, *nicht* $\frac{p-1}{\delta}$te Stammwurzeln. Nimmt man also von allen den Werthen von r in (1.) alle diejenigen Potenzen, deren Exponenten x in $\frac{p-1}{\delta}$ *aufgehen*, so sind die r, welche in (5.) $R=1$ geben, von den r in (1.) *auszuschliefsen;* die übrig bleibenden r sind $\frac{p-1}{\delta}$te *Stammwurzeln*; gemäfs (IV.).

Anm. *K.* Die gegenwärtigen Sätze beruhen auf (§. 40. 54. und 55.), und nächstdem auf den besondern Erwägungen in dem Beweise.

§. 65.

Lehrsatz.

I. *Diejenigen von den Zahlen* 1, 2, 3, 4, ... z (z = 2 *ausgenommen*), *welche mit* z *keinen Theiler* > 1 *gemein haben, sind immer paarweise vorhanden, und die Summe jedes solchen Paares ist* = z.

II. *Die Summe aller zu* z *theilerfremden Zahlen* (z = 2 *ausgenommen*) *geht mit* z *auf.*

III. *Das Product jeder zwei zu einander theilerfremden Theiler einer beliebigen Zahl* z *kann kleiner, aber nicht gröfser sein als* z.

Beispiel. Es sei z = 180. Die zu dieser Zahl theilerfremden Zahlen sind

1. { 1 7 11 13 17 19 23 29 31 37 41 43 47 49 53 59 61 67 71 73 77 79 83 89
179 173 169 167 163 161 157 151 149 143 139 137 133 131 127 121 119 113 109 107 103 101 97 91.

Die Zahlen stehen paarweise unter einander; und von jedem Paar ist die Summe $= z$; gemäfs (I.).

Die Summe aller der Zahlen (1.) ist 4320; was mit $z = 180$ aufgeht; gemäfs II.

Die verschiedenen *Theiler* von z sind folgende:

2. 1 2 3 4 5 6 9 10 12 15 18 20 30 36 45 60 90.

Die Producte der zu einander *theilerfremden* Theiler sind

$$3.\quad \begin{cases} 2.\,3 = 6, & 2.\,5 = 10, & 2.\,9 = 18, & 2.15 = 30, & 2.45 = 90; \\ 3.\,4 = 12, & 3.\,5 = 15, & 3.10 = 30, & 3.20 = 60; \\ 4.\,5 = 20, & 4.\,9 = 36, & 4.15 = 60, & 4.45 = 180; \\ 5.\,6 = 30, & 5.12 = 60, & 5.36 = 180; \\ 9.10 = 90, & 9.20 = 180. \end{cases}$$

Keins dieser Producte ist gröfser als $z = 180$; gemäfs (III.).

Beweis. *A.* Wenn die Zahl $a > 0 < z$ zu z theilerfremd ist, so ist es nothwendig auch $z - a = b$: denn ginge eine Zahl > 1 in b und z zugleich auf, so ginge sie auch nothwendig in a auf (§. 18.). Also ist zu jeder zu z theilerfremden Zahl a eine andere $b > 0 < z$ vorhanden, die ebenfalls mit z keinen Theiler > 1 gemein hat. Die zu z theilerfremden Zahlen > 0 und $< z$ sind also immer *paarweise* vorhanden, und die Summe jedes solchen Paares a und b ist $a + b = z$; gemäfs (I.).

B. Da die Summe jedes *Paares* der zu z theilerfremden Zahlen z ausmacht, so ist die Summe *aller* ein *Vielfaches* von z, und geht also mit z auf; gemäfs (II.).

C. a. Es seien δ_1 und δ_2 zwei zu einander *theilerfremde* Theiler von z, und es sei, wenn es möglich ist, ihr Product $\delta_1\delta_2 > z$, also etwa

$$4.\quad \delta_1\delta_2 = nz + r;$$

wo durch n immer $r < z$ gemacht werden kann, weswegen denn $r < \delta_1\delta_2$ vorausgesetzt werden darf.

b. Da nun z sowohl mit δ_1, als mit δ_2 aufgehen soll, so mufs nach (§. 18.) in (4.) auch nothwendig r sowohl mit δ_1, als mit δ_2, also nach (§. 26.) mit $\delta_1\delta_2$ aufgehen. Aber r ist nothwendig $< \delta_1\delta_2$ (*a.*), also kann r nur 0 sein und folglich nur

$$5.\quad \delta_1\delta_2 = nz$$

gesetzt werden.

c. Kann nun $n > 1$ sein, so mufs vermöge (5.) n entweder in δ_1 oder in δ_2 aufgehen; oder auch irgend ein *Theiler* n_1 von n mufs in δ_1, der

andere Theiler n_2, welcher $n_1 n_2 = n$ giebt, mufs in δ_2 aufgehen. Ist $n_1 = n_2$, so mufs n selbst in δ_1 oder δ_2 aufgehen, denn δ_1 und δ_2 haben nach der Voraussetzung keinen Theiler $n_1 = n_2 > 1$ gemein.

d. Also zunächst für *gleiche* Theiler von n mufs die Gleichung (5.) so wie sie ist stattfinden. Geht dann n etwa in δ_1 auf, so folgt daraus

$$6. \quad \frac{\delta_1}{n}.\delta_2 = z.$$

Dieses durch δ_1 dividirt giebt

$$7. \quad \frac{\delta_2}{n} = \frac{z}{\delta_1},$$

hier ist $\frac{z}{\delta_1}$ eine *ganze* Zahl, $\frac{\delta_2}{n}$ aber *nicht*, weil δ_1 und δ_2 den Theiler $n > 1$ *nicht* gemein haben. Also kann für *gleiche* Theiler von n, (7.) nur für $n = 1$ stattfinden, und also n nicht > 1, mithin in (5.) $\delta_1\delta_2$ nicht $> z$ sein.

e. Für *ungleiche* Theiler n_1 und n_2 von n würde (5.)

$$8. \quad \delta_1\delta_2 = n_1 n_2 z$$

geben, und, wenn nun n_1 in δ_1, n_2 in δ_2 aufgehend angenommen wird,

$$9. \quad \frac{\delta_1}{n_1}.\frac{\delta_2}{n_2} = z.$$

Dies durch δ_1 oder δ_2 dividirt giebt

$$10. \quad \frac{\delta_2}{n_1 n_2} = \frac{z}{\delta_1} \quad \text{und} \quad \frac{\delta_1}{n_1 n_2} = \frac{z}{\delta_2},$$

hier sind $\frac{z}{\delta_1}$ und $\frac{z}{\delta_2}$ *ganze* Zahlen, $\frac{\delta_2}{n_1 n_2}$ und $\frac{\delta_1}{n_1 n_2}$ aber sind es *nicht*, weil δ_2 zwar mit n_2, aber nicht mit dem Theiler n_1 von δ_1, und δ_1 zwar mit n_1, aber nicht mit dem Theiler n_2 von δ_2 aufgeht. Die erste Gleichung (10) findet also nur Statt für $n_1 = 1$ und die zweite nur für $n_2 = 1$, mithin (8.) nur für $n_1 n_2$ oder $n = 1$. Also auch in diesem Fall kann in (5.) n nicht gröfser sein als 1, und folglich $\delta_1\delta_2$ nicht gröfser als z. Also kann überhaupt $\delta_1\delta_2$ nicht gröfser als z sein; gemäfs (III.).

§. 66.

Lehrsatz.

Wenn p *eine ungerade Stammzahl ist, so ist*

I. *Für jede Stammwurzel* z_δ *aus* 1 *zu* p *mit geradem Exponenten* δ, *also, da* p—1 *immer gerade ist, auch für jede* p—1*te oder Hauptstammwurzel:*

$$1. \quad z_\delta^{\frac{1}{2}\delta} = \text{Ⓜ}p - 1.$$

Aber nur allein für den Exponenten $\frac{1}{2}\delta$, *und für keinen andern Exponenten* $<\delta$, *ist zu* p *der Rest* $=-1$.

II. *Von allen Stammwurzeln* z_δ *aus* 1 *zu* p *mit ungeradem Exponenten* δ *giebt keine der Potenzen* $z_\delta^1, z_\delta^2, z_\delta^3, \ldots$ *bis* z_δ^δ *zu* p *den Rest* -1.

III. *a. Alle Hauptstammwurzeln aus* 1 *zu* p *sind Nichtquadratreste zu* p.

b. Alle $\frac{p-1}{\lambda}=\delta$*ten Stammwurzeln aus* 1 *zu* p *sind, wenn* λ *eine Stammzahl ist,* λ*te Reste zu* p, *das heifst Werthe von* r *in*

$$2.\quad x^\lambda = \mathfrak{G}p+r.$$

c. Alle $\frac{p-1}{x}=\delta$*ten Stammwurzeln aus* 1 *zu* p *sind, wenn* x *nicht eine Stammzahl ist,* λ*te Reste* r *zu* p *in* (2.), *wenn* λ *eine der Stammzahlen ist, die in* x *aufgehen.*

d. Nur dann sind alle Nichtquadratreste zu p, $p-1$ *ausgenommen, Hauptstammwurzeln aus* 1 *zu* p, *wenn* $p-1$ *mit keiner andern Stammzahl als* 2 *und mit* $\frac{1}{2}(p-1)$ *aufgeht. Sonst nicht.*

e. Für kein x *sind in*

$$3.\quad z^x = \mathfrak{G}p+r$$

alle r *für* $z=1,2,3,4,\ldots p-1$, $\frac{p-1}{x}=\delta$*te Stammwurzeln.*

IV. *Für jede Stammzahl* p *und für jedes* δ *sind die* δ*ten Stammwurzeln aus* 1 *zu* p *für ein und dasselbe* δ *entweder sämmtlich Quadratreste, oder sämmtlich Nichtquadratreste; nicht zum Theil Quadratreste, zum Theil Nichtquadratreste. Desgleichen ist das Product jeder geraden Zahl von* δ*ten Stammwurzeln aus* 1 *zu* p *für jedes* p *und* δ *ein Quadratrest zu* p.

V. *Wenn man für eine Stammwurzel* z_δ *aus* 1 *zu* p *mit geradem Exponenten* δ, *also auch für eine Hauptstammwurzel,*

$$4.\quad z_\delta^x = \mathfrak{G}p+r$$

setzt, wo $x<\frac{1}{2}\delta$, *so ist*

$$5.\quad z_\delta^{\frac{1}{2}\delta+x} = \mathfrak{G}p-r;$$

so dafs man also die Reste zu allen Potenzen $z_\delta^{\frac{1}{2}\delta+x}$ *findet, wenn man diejenigen zu* z^x *von* p *abzieht.*

VI. *Ist der Exponent* δ *einer Stammwurzel* z_δ *aus* 1 *zu* p *eine ungerade Zahl, so ist* $p-z_\delta$ *eine* 2δ*te Stammwurzel aus* 1 *zu* p.

VII. *Wenn in*

$$6. \quad z^x = \mathfrak{S}p + r$$

x die Theiler von δ bezeichnet, so dafs also x auch δ selbst sein kann: wenn ferner δ gerade ist, und der Rest r *für* $x = \frac{1}{2}\delta$ *ist gleich* -1, *für alle andern x dagegen, die nur in δ und nicht in* $\frac{1}{2}\delta$ *aufgehen, weder* $+1$, *noch* -1, *so ist* z *nothwendig eine δte Stammwurzel aus* 1 *zu* p.

Findet nicht beides zugleich Statt, so ist z *nicht eine δte Stammwurzel aus* 1 *zu* p.

VIII. *a. Wenn der Exponent δ einer δten Stammwurzel* z_δ *aus* 1 *zu* p *mit* 4 *aufgeht, so ist auch* p—z *eine δte Stammwurzel aus* 1 *zu* p.

b. Geht δ nur mit 2, *nicht mit* 4 *auf, so ist* p—z *eine* $\frac{1}{2}\delta$*te Stammwurzel aus* 1 *zu* p; *so dafs es also für alle mit* 2 *und nicht mit* 4 *aufgehenden δ eben so viele* $\frac{1}{2}\delta$*te als δte Stammwurzeln aus* 1 *zu* p *giebt.*

IX. *Wenn* z_δ *eine δte und* z_ε *eine εte Stammwurzel aus* 1 *zu* p *ist, und δ und ε sind zu einander theilerfremd, so ist in*

$$7. \quad z_\delta . z_\varepsilon = \mathfrak{S}p + r,$$

wenn $r > 1$ *ist,* r *eine δεte Stammwurzel aus* 1 *zu* p, *und* δε *ist nie gröfser als* p—1 (§. 65. III.).

X. *Wenn in*

$$8. \quad z_\delta^x = \mathfrak{S}p + r,$$
$$9. \quad x^\lambda = \mathfrak{S}p + z_\delta,$$

z *eine δte Stammwurzel aus* 1 *zu* p *ist, und unter den Resten* r *in* (8.), *für die verschiedenen* $x = 1, 2, 3, \ldots \delta - 1$, *kommt weder* $x - \mathfrak{S}p$, *noch* $x^2 - \mathfrak{S}p$, *noch* $x^3 - \mathfrak{S}p$, ..., *bis zu* $x^{\lambda-1} - \mathfrak{S}p$ *vor, so ist* x *eine λxte Stammwurzel aus* 1 *zu* p.

Beispiele. Aus Taf. I. Zu I. Für die δ = 4te Stammwurzel 11 ist $11^{\frac{1}{2}\delta} = 11^2 = \mathfrak{S}p + 60 = \mathfrak{S}p - 1$. Für die δ = 6te Stammwurzel 14 ist $14^{\frac{1}{2}\delta} = 14^3 = \mathfrak{S}p + 60 = \mathfrak{S}p - 1$. Für die δ = 20te Stammwurzel 37 ist $37^{\frac{1}{2}\delta} = 37^{10} = \mathfrak{S}p + 60 = \mathfrak{S}p - 1$, u. s. w. Kein anderer aber als der Exponent $\frac{1}{2}\delta$ giebt zu p den Rest 60 oder —1.

Zu II. Zu der δ = 3ten Stammwurzel 13 sind die Reste 13 und 47; zu der δ = 5ten Stammwurzel 34 sind die Reste 34, 58, 20 und 9; für die δ = 15te Stammwurzel 16 sind die Reste 16, 12, 9, 22, 47, 20, 15, 57, 58, 13, 25, 34, 56 und 42, u. s. w. Keiner dieser Reste ist 60 oder —1; gemäfs (II.).

Zu III. Die Zahlen in der *zweiten* horizontalen Zeile der Tafel sind die *Quadratreste* zu p. Unter ihnen findet sich *keine* der Hauptstammwurzeln 2, 6, 7, 10, 17 etc.; also sind alle Hauptstammwurzeln *Nichtquadratreste* zu p; gemäfs (III. *a.*).

Dagegen finden sich alle die $\frac{p-1}{2} = 30$ten Stammwurzeln 4, 5, 19, 36 etc. unter den Zahlen der *zweiten* horizontalen Zeile der Tafel, und sind also alle *zweite* oder *Quadratreste* zu p. Die Zahlen der *dritten* horizontalen Zeile sind die $\lambda = 3$*ten Reste* zu p. Unter ihnen befinden sich in $\frac{p-1}{3} = 20$ten Stammwurzeln 8, 23, 24 etc. Die Zahlen der *fünften* horizontalen Zeile sind die $\lambda = 5$*ten Reste* zu p. Unter ihnen befinden sich die $\frac{p-1}{5} = 12$ten Stammwurzeln 21, 29, 32 etc. Ferner befinden sich z. B. die $\frac{p-1}{x} = \frac{p-1}{6} = 10$ten Stammwurzeln 3, 27, 41 .... unter den Zahlen der 3ten horizontalen Zeile; u. s. w.; gemäfs (III. *b.* und *c.*). Aber *nicht alle* Zahlen, die in der zweiten horizontalen Zeile *nicht* stehen, also nicht alle Nichtquadratreste, sind Hauptstammwurzeln; und *nicht alle* Zahlen der 3ten, 5ten Zeile etc. sind $\frac{p-1}{3}$, $\frac{p-1}{5}$, $\frac{p-1}{6}$te etc. Stammwurzeln.

Zu III. *d.* giebt die im 9ten Bande dieses Journals S. 36 — 53 abgedruckte Tafel Beispiele. Für $p = 23$ geht $p-1$ nur mit den Stammzahlen 2 und $11 = \frac{1}{2}(p-1)$ auf. Die *Nichtquadratreste* zu $p = 23$ sind 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 und 22. Alle diese Zahlen, $p-1 = 22$ ausgenommen, sind Hauptstammwurzeln aus 1 zu $p = 23$.

Hier in Tafel I. sind z. B. für $x = 6$ die verschiedenen Werthe von r in (3.) folgende: 1, 3, 9, 20, 27, 34, 41, 52, 58 und 60. Nicht diese Zahlen *alle*, sondern nur die vier: 3, 27, 41 und 52 sind $\frac{p-1}{x} = \frac{60}{6} = 10$te Stammwurzeln aus 1 zu p; gemäfs (III. *e.*).

Zu IV. Nach Tafel I. sind z. B. die 20ten Stammwurzeln 8, 23, 24, 28, 33, 37, 38 und 53 *sämmtlich Nichtquadratreste;* denn sie finden sich nicht unter den Zahlen der zweiten horizontalen Zeile der Tafel. Dagegen die 15ten Stammwurzeln 12, 15, 16, 22, 25, 42, 56 und 57 sind *sämmtlich Quadratreste;* gemäfs (IV.).

Zu V. Für die $\delta = 10$te Stammwurzel $z = 27$ aus 1 zu $p = 61$ ist z. B. $z^r = z^3 = \mathfrak{G}p+41$, also in (4.) $r = 41$, und $z^{\frac{1}{2}\delta+\alpha} = z^8$ ist $= \mathfrak{G}p+20 = \mathfrak{G}p-41 = \mathfrak{G}p-r$. Für die $\delta = 30$te Stammwurzel $z = 39$ ist z. B.

$z^{\varkappa} = z^{11} = \mathfrak{G}p + 19$, also $r = 19$; $z^{\frac{1}{2}\delta+\varkappa} = z^{26}$ ist $= \mathfrak{G}p + 42 = \mathfrak{G}p - 19$ $= \mathfrak{G}p - r$. Für die Hauptstammwurzel $z = 43$ ist z. B. $z^{\varkappa} = z^{14} = \mathfrak{G}p + 4$, also $r = 4$; und $z^{\frac{1}{2}\delta+\varkappa} = z^{44}$ ist $= \mathfrak{G}p + 57 = \mathfrak{G}p - 4 = \mathfrak{G}p - r$ etc.; gemäfs (V.).

Zu VI. $z = 13$ ist eine Stammwurzel aus 1 zu p mit der ***ungeraden*** Zahl 3 zum Exponenten; und $p - z = 48$ ist eine $2\delta = 6$te Stammwurzel aus 1 zu p. $z = 20$ ist eine Stammwurzel mit der ***ungeraden*** Zahl 5 zum Exponenten; und $p - z = 41$ ist eine $2\delta = 10$te Stammwurzel aus 1 zu p; gemäfs (VI.).

Zu VII. Von $\delta = 20$ sind die Theiler $\varkappa = 1, 2, 4, 5$ und 10. Davon ist derjenige, welcher ***nur*** in δ, ***nicht*** in $\frac{1}{2}\delta = 10$ aufgeht, 4. Für $z = 28$ ist $z^{\frac{1}{2}\delta} = z^{10} = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$ und $z^{4} = \mathfrak{G}p + 20$. Also ist r in (6.) $= -1$ für $\varkappa = \frac{1}{2}\delta$ und weder $+1$ noch -1 für das $\varkappa$, welches nicht in $\frac{1}{2}\delta$ aufgeht; und $z = 28$ ist eine 20te Stammwurzel aus 1 zu p.

Dagegen ist für $z = 11$ zwar $z^{10} = \mathfrak{G}p + 60 = \mathfrak{G}p - 1$, aber z^{4} ist $= \mathfrak{G}p + 1$, und $z = 11$ ist ***nicht*** eine 20te Stammwurzel; gemäfs (VII.).

Zu VIII. Für $\delta = 20$ sind $z_{\delta} = 8, 23, 24, 28$ Stammwurzeln aus 1 zu p. δ geht ***mit*** 4 ***auf***, und $p - (8, 23, 24, 28) = 53, 38, 37$ und 33 sind ebenfalls 20te Stammwurzeln aus 1 zu p; gemäfs (VIII. *a*.).

Die $\delta = 30$ten Stammwurzeln aus 1 zu p sind $z = 4, 5, 19, 36, 39, 45, 46$ und 49. Hier geht δ ***nur mit*** 2, ***nicht*** mit 4 auf, und $p - (4, 5, 19, 36, 39, 45, 46, 49)$ $= 57, 56, 42, 25, 22, 16, 15$ und 12 sind die $\frac{1}{2}\delta = 15$ten Stammwurzeln aus 1 zu p; gemäfs (VIII. *b*.).

Zu IX. $z_{\delta} = 11$ ist eine $\delta = 4$te und $z_{\varepsilon} = 42$ eine $\varepsilon = 15$te Stammwurzel aus 1 zu p. δ und ε sind zu einander theilerfremd, und (7.) giebt hier $z_{\delta} z_{\varepsilon} = 11 . 42 = 462 = \mathfrak{G}p + 35$, also $r = 35$; und dieses $r = 35$ ist eine $4 . 15 = 60$te oder Hauptstammwurzel; gemäfs (IX.).

Zu X. $z_{\delta} = 22$ ist eine $\delta = 15$te Stammwurzel aus 1 zu p, und $12^{2} = \mathfrak{G}p + 22$, also in (9.) $x = 12$. Die Reste r in (8.) zu $z = 22$ sind für $x = 1, 2, 3, \ldots 14$, $r = 22, 57, 34, 16, 47, 58, 56, 12, \ldots$ etc. Unter denselben ***kommt*** $x = 12$ ***vor***, also ist $x = 12$ ***nicht*** eine $\lambda\delta = 4 . 15 = 60$te Stammwurzel aus 1 zu p. In der That ist 12 nur eine 12te Stammwurzel aus 1 zu p. Dagegen ist $z_{\delta} = 29$ eine $\delta = 12$te Stammwurzel aus 1 zu p, und $6^{5} = \mathfrak{G}p + 29$, also in (9.) $x = 6$. Die Reste r in (8.) zu $z = 29$ sind 29, 48, 50, 47, 21, 60, 32, 13, 11, 14, 40. Unter denselben kommt weder $x = 6$,

noch $x^2 = \mathfrak{G}p + 36$, noch $x^3 = \mathfrak{G}p + 33$, noch $x^4 = \mathfrak{G}p + 15$ vor; also mufs $x = 6$ eine $5.12 = 60$te Stammwurzel aus 1 zu p sein; was auch der Fall ist; gemäfs (X.).

Beweis von I. *A.* Für eine δte Stammwurzel aus 1 zu p ist $z^\delta = \mathfrak{G}p + 1$ oder

$$10.\quad z_\delta^\delta - 1 = \mathfrak{G}p.$$

Dieses giebt, wenn δ *gerade*, also $\frac{1}{2}\delta$ eine *ganze* Zahl ist,

$$11.\quad (z_\delta^{\frac{1}{2}\delta} - 1)(z_\delta^{\frac{1}{2}\delta} + 1) = \mathfrak{G}p:$$

also mufs p entweder in $z_\delta^{\frac{1}{2}\delta} - 1$, oder in $z_\delta^{\frac{1}{2}\delta} + 1$ *aufgehen*, das heifst, es mufs

$$12.\quad \text{entweder } z_\delta^{\frac{1}{2}\delta} = \mathfrak{G}p + 1,$$

$$13.\quad \text{oder } z_\delta^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$$

sein. Das Erste (12.) kann nicht sein, denn sonst gäbe nicht erst die δte, sondern schon die $\frac{1}{2}\delta$te Potenz von z_δ zu p den Rest $+1$, und z_δ wäre also keine δte *Stammwurzel.* Mithin mufs die Gleichung (13.) stattfinden; und diese ist die (1.) des Lehrsatzes.

B. Wäre noch für einen andern Exponenten als $\frac{1}{2}\delta$, z. B. für den Exponenten $\varepsilon < \delta$,

$$14.\quad z_\delta^\varepsilon = \mathfrak{G}p - 1,$$

so wäre

$$15.\quad z_\delta^{2\varepsilon} = \mathfrak{G}p + 1.$$

Aber 2ε ist *nicht* $= \delta$, sondern entweder kleiner oder gröfser als δ, jedoch $< 2\delta$. Setzt man für den zweiten Fall $2\varepsilon = \delta + \varkappa$, wo nun $\varkappa < \delta$ ist, so wäre

$$16.\quad z_\delta^{2\varepsilon} = z_\delta^{\delta+\varkappa} = z_\delta^\delta z_\delta^\varkappa = (\mathfrak{G}p + 1) z_\delta^\varkappa = \mathfrak{G}p + z_\delta^\varkappa,$$

also müfste, wenn nach (15.) $z_\delta^{2\varepsilon} = \mathfrak{G}p + 1$ sein sollte, $\mathfrak{G}p + z_\delta^\varkappa = \mathfrak{G}p + 1$ oder

$$17.\quad z_\delta^\varkappa = \mathfrak{G}p + 1$$

sein. Aber für *keinen* Exponenten, der kleiner ist als δ, ist der Rest der Potenz zu p gleich $+1$, weil z_δ eine δte *Stammwurzel* sein soll. Also kann die Gleichung (15.) weder für $2\varepsilon < \delta$, noch, in der Form (17.), für $2\varepsilon > \delta$ $< 2\delta$ stattfinden, und folglich auch nicht die Gleichung (14.), und es giebt mithin *kein* anderer Exponent ε, als $\frac{1}{2}\delta$, für die δte Stammwurzel z_δ, $z_\delta^\varepsilon = \mathfrak{G}p - 1$; gemäfs (I.).

Bew. von II. *C.* Ist δ *ungerade*, und wäre für einen andern Exponenten als δ, z. B. für $\varepsilon < \delta$, $z_\delta^\varepsilon = \mathfrak{G}p - 1$, so müfste wieder, wie in (15.), $z_\delta^{2\varepsilon} = \mathfrak{G}p + 1$ sein; und da 2ε *nicht* $= \delta$ sein kann, sondern entweder $< \delta$

oder $>\delta<2\delta$ ist, so folgt, ganz wie in (*B.*), dafs für *kein* $\varepsilon<\delta$ die δte Stammwurzel z_δ, $z_\delta^\varepsilon = \mathfrak{G}p-1$ geben kann; gemäfs (II.).

Bew. von III. *a.* *D.* Die *Hauptstammwurzeln* z_{p-1}, für welche

$$18.\quad z_{p-1}^{\frac{p-1}{1}} = \mathfrak{G}p+1$$

sein mufs, können nicht unter den *Quadratresten* r zu p sein, für welche $z^2=\mathfrak{G}p+r$ ist: denn nach (§. 49. 1.) ist für die *Quadratreste* r schon

$$19.\quad r^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1,$$

also *schon* ihre $\frac{1}{2}(p-1)$te Potenz läfst zu p den Rest 1; was für $p-1$te Stammwurzeln nicht der Fall ist. Da es aber nun *jedenfalls* Hauptstammwurzeln *giebt,* so können sich dieselben nur unter den *Nichtquadratresten* ϱ befinden; gemäfs (III. *a.*).

Bew. von III. *b.* *E.* Die Gleichung (2.) giebt, wenn man die $\frac{p-1}{\lambda}$te Potenz nimmt,

$$20.\quad z^{\frac{p-1}{\lambda}\cdot\lambda} = z^{p-1} = \mathfrak{G}p+r^{\frac{p-1}{\lambda}}$$

und, da für *jedes* z nach dem Fermatschen Lehrsatz (§. 40.) $z^{p-1}=\mathfrak{G}p+1$ ist,

$$21.\quad r^{\frac{p-1}{\lambda}} = \mathfrak{G}p+1.$$

Dieses ist eine der Bedingungen für die $\frac{p-1}{\lambda}=\delta$ten Stammwurzeln z_δ: also müssen sich alle $\frac{p-1}{\lambda}=\delta$ten Stammwurzeln z_δ unter den λten Resten r in (2.) finden; gemäfs (III. *b.*).

Bew. von III. *c.* *F.* Wenn z eine $\delta=\frac{p-1}{\varkappa}$te Stammwurzel aus 1 zu p sein soll, so mufs

$$22.\quad z^{\frac{p-1}{\varkappa}} = \mathfrak{G}p+1$$

sein; also: wenn λ eine der in $\varkappa$ *aufgehenden* Stammzahlen ist, und man setzt etwa

$$23.\quad \varkappa = \mu\lambda,$$

so mufs

$$24.\quad z^{\frac{p-1}{\mu\lambda}} = \mathfrak{G}p+1,$$

also auch

$$25.\quad z^{\frac{p-1}{\lambda}} = (\mathfrak{G}p+1)^\mu = \mathfrak{G}p+1$$

sein. Diese Bedingung erfüllen die r in (2.) gemäfs (21.). Also *müssen* sich alle $\delta=\frac{p-1}{\varkappa}$ten Stammwurzeln unter den λten Resten r in (2.) finden.

Bew. von III. *d.* *G.* *α.* Es giebt immer $\frac{1}{2}(p-1)$ *Nichtquadratreste* (§. 45. III.), und nach (§. 63. I.) giebt es so viele *Hauptstammwurzeln* als Zahlen >0 und $<p$ zu $p-1$ theilerfremd sind.

β. Nun ist $p-1$ *immer gerade*, also sind die $\frac{1}{2}(p-1)$ Zahlen 2, 2.2, 3.2, 4.2, ... $\frac{1}{2}(p-1).2=p-1$ zu $p-1$ *nicht* theilerfremd; sondern haben damit den Theiler $2>1$ gemein. Es bleiben von den gesammten $p-1$ Zahlen $1, 2, 3, 4, \ldots\ldots p-1$ nur die $\frac{1}{2}(p-1)$ *ungeraden* Zahlen 1, 3, 5, 7, ... $p-1-1$ übrig, die zu $p-1$ theilerfremd sein können. Geht nun $p-1$ nur mit den Stammzahlen 2 und $\frac{1}{2}(p-1)$ auf, so sind sie es mit Ausnahme von $p-1$ *wirklich;* denn keine von ihnen geht mit 2 auf. Also giebt es alsdann wirklich $\frac{1}{2}(p-1)-1$ Hauptstammwurzeln, so viele als Nichtquadratreste, mit Ausnahme von $p-1$. Und da nun alle Hauptstammwurzeln Nichtquadratreste sind, so sind alsdann alle Nichtquadratreste, mit Ausnahme von $p-1$, Hauptstammwurzeln.

γ. Geht dagegen $p-1$, aufser mit 2, noch mit andern, also noch mit einer oder mehreren *ungeraden* Stammzahlen q_1, q_2, ... $<p$ auf, so befinden sich dieselben nothwendig unter den $\frac{1}{2}(p-1)$ *ungeraden* Zahlen 1, 3, 5, 7, ... $p-2$, die allein noch zu $p-1$ theilerfremd sein konnten; denn diese ungeraden Zahlen sind diejenigen $<p$ *alle*, welche es giebt. Es gehen also alsdann schon q_1, q_2, ... von jenen $\frac{1}{2}(p-1)$ ungeraden Zahlen ab, und folglich giebt es dann *weniger* oder $\frac{1}{2}(p-1)$ zu $p-1$ theilerfremde Zahlen >0 und $<p$, und mithin auch weniger Hauptstammwurzeln. Mithin sind alsdann *nicht alle* Nichtquadratreste Hauptstammwurzeln; gemäfs (III. *d.*).

Bew. von III. *e.* Nach (§. 54. I.) hat r in (3.) $\frac{p-1}{x}=\delta$ *verschiedene* Werthe. Andrerseits ist nach (§. 63. I.) die Anzahl der $\frac{p-1}{x}=\delta$ten Stammwurzeln aus 1 zu p der Anzahl der zu δ *theilerfremden* Zahlen gleich. Letztere ist *immer* $<\delta$, selbst wenn δ eine *Stammzahl* ist; denn selbst dann sind erst die $\delta-1$ Zahlen 1, 2, 3, 4, ... $\delta-1$ zu δ *theilerfremd.* Also sind für *kein* x *alle* r in (3.) $\frac{p-1}{x}=\delta$te Stammwurzeln; gemäfs (III. *e.*).

Bew. von IV. *H.* Alle $\delta=\frac{p-1}{x}$ten Stammwurzeln x_δ, für *denselben* Exponenten δ, finden sich nach (III. *c.*) unter den Resten r in $z^\lambda=\mathfrak{G}p+r$ für *denselben* Exponenten λ, der eine von den in x aufgehenden *Stammzahlen* ist. Diese Reste r sind entweder *Quadratreste*, oder *Nichtquadratreste;*

denn andere Zahlen $>0 < p$ giebt es nicht. Ist nun eine der δten Stammwurzeln ein r, welches ein *Quadratrest*, also ein Rest *für* $\lambda = 2$ *ist*, so sind es auch alle andern δten Stammwurzeln; *denn alle* finden sich unter den r für das *gleiche* λ. Ist eine der δten Stammwurzeln z_1 ein r, welches ein *Nichtquadratrest* ist, so kann keine andere δte Stammwurzel ein *Quadratrest* sein; denn sonst wären es, wie so eben bemerkt, auch *alle andern*, und folglich auch z_1.

Also, wenn eine δte Stammwurzel ein *Quadratrest* ist, so sind es auch alle andern; und wenn eine derselben ein *Nichtquadratrest* ist, sind es ebenfalls alle übrigen.

Das Product jeder *geraden* Anzahl von Quadratresten und Nichtquadratresten ist nach (§. 52. I. und II.) ein *Quadratrest:* also ist das Product jeder *geraden* Anzahl von δten Stammwurzeln für jedes p und δ ein *Quadratrest;* gemäfs (IV.).

Bew. von V. *F.* Nach (I.) ist für jedes *gerade* δ

$$26. \quad z_\delta^{\frac{1}{2}\delta} = \mathfrak{G}p - 1.$$

Setzt man nun, wie in (2.),

$$27. \quad z_\delta^{x} = \mathfrak{G}p + r,$$

so ergiebt sich, wenn man (26.) mit (27.) multiplicirt,

$$28. \quad z_\delta^{\frac{1}{2}\delta + x} = \mathfrak{G}p - r = \mathfrak{G}p + (p - r);$$

gemäfs (V.).

Bew. von VI. *G.* Es ist

$$29. \quad (p-z)^{2\delta} = \mathfrak{G}p + (-z)^{2\delta} = \mathfrak{G}p + z^{2\delta},$$

indem 2δ *immer* gerade ist. Ist nun z eine δte Stammwurzel aus 1 zu p, so ist

$$30. \quad z_\delta^{\delta} = \mathfrak{G}p + 1.$$

Aber es ist

$$31. \quad (p - z_\delta)^{\delta} = \mathfrak{G}p + (-z)^{\delta},$$

also ist, für ein *ungerades* δ,

$$32. \quad (p - z_\delta)^{\delta} = \mathfrak{G}p - z_\delta^{\delta} = \mathfrak{G}p - 1 \ (30.),$$

und folglich *kann* nach (I.) $p - z_\delta$ eine 2δte Stammwurzel sein; denn ist sie eine solche, so mufs nach (I.) $(p - z_\delta)^{\delta} = \mathfrak{G}p - 1$ sein; was nach (32.) der Fall ist.

H. Es ist aber auch, für jeden Exponenten $x < \delta$,

$$33. \quad (p - z_\delta)^{x} = \mathfrak{G}p + (-z_\delta)^{x} = \mathfrak{G}p \pm z_\delta^{x},$$

je nachdem x gerade oder ungerade ist. Könnte nun für $x < \delta$, $(p - z_\delta)^{x} = \mathfrak{G}p \pm 1$ sein, so müfste zufolge (33.)

$$34. \quad z_\delta^x = \mathfrak{G}p \pm 1$$

sein. Dieses ist nicht der Fall; denn *keine* niedrigere Potenz als δ von der δten Stammwurzel z_δ giebt zu p den Rest $+1$, was auch δ sein mag; und wenn δ *ungerade* ist, giebt auch keine niedrigere Potenz als δ nach (II.) den Rest -1 zu p: also kann r in

$$35. \quad (p-z_\delta)^x = \mathfrak{G}p + r$$

für kein $x < \delta$ weder $+1$ noch -1 sein.

I. Multiplicirt man nun (35.) mit (32.), so ergiebt sich

$$36. \quad (p-z_\delta)^{\delta+x} = \mathfrak{G}p - r:$$

also kann auch keine Potenz von $p-z_\delta$, deren Exponent $>\delta$ und $<2\delta$ ist, zu p weder $+1$ noch -1 zum Rest geben. Mithin kann überhaupt keine Potenz von $p-z_\delta$, deren Exponent >0 und $<2\delta$ ist, zu p den Rest $+1$ lassen; die δte Potenz von $p-z_\delta$ läfst aber nach (32.) zu p den Rest -1: mithin ist $p-z_\delta$ nothwendig eine 2δte Stammwurzel; gemäfs (VI.).

Bew. von VII. *K.* Wenn für einen *geraden* Theiler δ von $p-1$

$$27. \quad z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$$

ist, so ist, die zweite Potenz genommen,

$$38. \quad z^\delta = \mathfrak{G}p + 1;$$

also *kann* alsdann dieses z eine δte Stammwurzel z_δ aus 1 zu p sein.

Aber wenn

$$39. \quad \delta = 2\lambda x$$

und schon

$$40. \quad z^x = \mathfrak{G}p + 1$$

oder auch

$$41. \quad z^x = \mathfrak{G}p - 1,$$

also $z^{2x} = \mathfrak{G}p + 1$ ist, so ist z nicht eine δte, sondern in dem Falle (40.) schon eine $x$te, und in dem Fall (41.) eine $2x$te Stammwurzel aus 1 zu p.

Dagegen giebt (40.), vermöge (39.), indem $\frac{1}{2}\delta = \lambda x$ ist,

$$42. \quad z^{\frac{1}{2}\delta} = z^{\lambda x} = (\mathfrak{G}p+1)^\lambda = \mathfrak{G}p + 1;$$

was der vorausgesetzten Gleichung (37.) widerspricht: also kann z für keinen Exponenten x, der in $\frac{1}{2}\delta$ aufgeht, eine $x$te Stammwurzel sein, sobald nach (37.) $z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$ ist.

L. Auch für kein anderes x, welches in δ *nicht* aufgeht, kann z eine $x$te Stammwurzel sein, sobald die Gleichung (37.) stattfindet. Denn gesetzt es sei

$$43. \quad \delta = nx + e,$$

wo $e > 0$ und $< x$, so ist, wenn z eine $x$te Stammwurzel, also

$$44. \quad z^x = \mathfrak{S}p+1$$

wäre,

$$45. \quad z^\delta = z^{nx+e} = (\mathfrak{S}p+1)^n z^e = \mathfrak{S}p+z^e.$$

Setzt man nun

$$46. \quad z^e = \mathfrak{S}p+\varepsilon,$$

so ist, wenn z eine $x$te *Stammwurzel* sein soll, also alle Potenzen mit Exponenten e, die $< x$ sind, *nicht* den Rest 1 geben, ε *nicht* $= 1$, und folglich, da, (46.) in (45.) gesetzt,

$$47. \quad z^\delta = \mathfrak{S}p+\varepsilon$$

giebt, in dieser Gleichung ε *nicht* $= 1$. Dieses widerspricht der vorausgesetzten Gleichung: also kann auch für kein x, welches in δ *nicht* aufgeht, z eine $x$te Stammwurzel sein, sobald (37.) Statt findet.

M. Eben so wenig kann für ein x, welches in $\frac{1}{2}\delta$ *nicht* aufgeht, z eine $x$te Stammwurzel sein; es sei denn, dafs x in δ aufginge. Denn setzt man

$$48. \quad \tfrac{1}{2}\delta = nx+e,$$

wo $e > 0$ und $< x$, so folgt, ganz wie in (*L.*),

$$49. \quad z^{\frac{1}{2}\delta} = \mathfrak{S}p+\varepsilon.$$

Es müfste also, damit (37.) erfüllt werde, $\varepsilon = -1$ sein können. Dieses kann nun zwar, wenn z eine $x$te Stammwurzel ist, in

$$50. \quad z^e = \mathfrak{S}p+\varepsilon \quad (46.)$$

allerdings der Fall sein, aber nach (1.) nur für $e = \frac{1}{2}x$; denn nur $z^{\frac{1}{2}x}$ giebt nach (1.) $\mathfrak{S}p-1$. Ist nun aber $e = \frac{1}{2}x$, so ist in (48.)

$$\tfrac{1}{2}\delta = nx+\tfrac{1}{2}x \text{ oder}$$

$$51. \quad \delta = nx+x,$$

und x mufs in δ *aufgehen*. Also kann auch für kein x, welches in $\frac{1}{2}\delta$ nicht aufgeht, z eine $x$te Stammwurzel aus 1 zu p sein; aufser wenn x in δ aufgeht.

N. Es kommt mithin *nur allein* auf die x an, *die in δ aufgehen;* nicht auf die x, nach (*K.*), *welche in $\frac{1}{2}\delta$ aufgehen;* und auch auf alle andern nicht.

Ist daher in der Gleichung (6.) für $x = \frac{1}{2}\delta$, $r = -1$, und für keines der x, welche in δ aufgehen, *ohne* Rücksicht auf diejenigen, welche in $\frac{1}{2}\delta$ aufgehen, weder $r = +1$, noch $r = -1$, so kann z für *keinen* niedrigeren Exponenten als δ eine Stammwurzel aus 1 zu p sein. Für $x = \delta$ dagegen ist, wegen $z^{\frac{1}{2}\delta} = \mathfrak{S}p-1$, nothwendig

$$52. \quad z^\delta = \mathfrak{S}p+1;$$

und folglich ist dann z *nothwendig* eine δte Stammwurzel aus 1 zu p; gemäfs (VII.).

O. Ist nicht $z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$, sondern

$$53. \quad z^{\frac{1}{2}\delta} = \mathfrak{G}p + r,$$

so ist

$$z^{\delta} = \mathfrak{G}p + r^2,$$

und r^2 ist nun $= +1$ für $r = +1$ oder $r = -1$: also ist dann z^{δ} *nicht* $= \mathfrak{G}p + 1$, und folglich z *nicht* eine δte Stammwurzel.

Werden andrerseits nicht die *übrigen* Bedingungen von (VII.) erfüllt, so ist z ebenfalls *nicht* eine δte Stammwurzel aus 1 zu p, wenn gleich $z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$ ist. Also kann nur, wenn *Beides* zugleich Statt findet: nemlich $z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1$ ist, und die übrigen Bedingungen in (VII.) erfüllt werden, z eine δte Stammwurzel aus 1 zu p sein.

Bew. von VIII. *P.* Geht δ mit 4 auf, so sind δ und $\frac{1}{2}\delta$ beide *gerade*. Für jedes *gerade* δ aber ist nach (1.), wenn z eine δte Stammwurzel aus 1 zu p ist,

$$55. \quad z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1.$$

Nun ist

$$56. \quad (p-z)^{\frac{1}{2}\delta} = \mathfrak{G}p + (-z)^{\frac{1}{2}\delta}$$

und, da *auch* $\frac{1}{2}\delta$ *gerade* ist,

$$57. \quad (p-z)^{\frac{1}{2}\delta} = \mathfrak{G}p + z^{\frac{1}{2}\delta} = \mathfrak{G}p - 1 \quad (55.).$$

Also *kann* dann $p - z$ eine δte Stammwurzel aus 1 zu p sein; denn (57.) giebt $(p-z)^{\delta} = \mathfrak{G}p + 1$.

Es läfst aber, wenn z eine δte Stammwurzel aus 1 zu p ist, keine *niedrigere* Potenz z^x von z als z^{δ} weder den Rest $+1$, noch, nach (I.), den Rest -1, sondern es ist

$$58. \quad z^x = \mathfrak{G}p + r,$$

wo r *nicht* $+1$ oder -1 ist. Dieses giebt

$$59. \quad (p-z)^x = \mathfrak{G}p + (-z)^x = \mathfrak{G}p \pm r:$$

folglich läfst auch von $p - z$ keine niedrigere als die δte Potenz zu p den Rest 1. Daher ist $p - z$ *nothwendig* eine δte Stammwurzel aus 1 zu p, wenn z eine solche ist; gemäfs (VII. *a.*).

Q. Geht δ mit 2, aber nicht mit 4 auf, so ist δ *gerade* und $\frac{1}{2}\delta$ *ungerade*. Die Gleichung (55.) bleibt dieselbe; aber (56.) giebt jetzt

$$60. \quad (p-z)^{\frac{1}{2}\delta} = \mathfrak{G}p - z^{\frac{1}{2}\delta} = \mathfrak{G}p + 1 \quad (55.):$$

also *kann* jetzt $p - z$ *eine* $\frac{1}{2}\delta$*te* Stammwurzel aus 1 zu p sein. Nun ist in (58.) r für alle $x < \delta$ nicht $+1$; blofs für $x = \frac{1}{2}\delta$ ist $r = -1$: also ist jetzt in (59.) r für alle $x < \delta$ nicht $+1$, und folglich ist $p - z$ *nothwendig* eine $\frac{1}{2}\delta$te Stammwurzel aus 1 zu p; gemäfs (VIII. *b.*).

Bew. von IX. *R. a.* Wenn z_δ eine δte und z_ε eine εte Stammwurzel aus 1 zu p ist, so ist

$$61.\quad z_\delta^\delta = \mathfrak{G}p+1 \text{ und}$$

$$62.\quad z_\varepsilon^\varepsilon = \mathfrak{G}p+1,$$

und keine niedrigere Potenz von z_δ als die δte, und keine niedrigere Potenz von z_ε als die εte giebt zu p den Rest 1.

b. Aus (61.), so wie aus (62.), folgt, wenn man von (61.) die εte und von (62.) die δte Potenz nimmt,

$$63.\quad z_\delta^{\delta\varepsilon} = \mathfrak{G}p+1 \text{ und } z_\varepsilon^{\delta\varepsilon} = \mathfrak{G}p+1,$$

also, Eins mit dem Andern multiplicirt,

$$64.\quad (z_\delta z_\varepsilon)^{\delta\varepsilon} = \mathfrak{G}p+1.$$

Daraus folgt, dafs das Product $z_\delta z_\varepsilon$ eine $\delta\varepsilon$*te Stammwurzel* aus 1 zu p sein *kann*.

c. Gesetzt nun, es wäre $z_\delta z_\varepsilon$ schon eine λte Stammwurzel aus 1 zu p, wo $\lambda < \delta\varepsilon$, so dafs schon

$$65.\quad (z_\delta z_\varepsilon)^\lambda = \mathfrak{G}p+1$$

wäre, dann aber keine niedrigere Potenz von $z_\delta z_\varepsilon$ als die λte zu p den Rest 1 gäbe, so müfste λ nothwendig in $\delta\varepsilon$ *aufgehen;* denn wäre es anders und

$$66.\quad \delta\varepsilon = \varkappa\lambda+\varrho,$$

wo $\varrho < \lambda$, so wäre

$$67.\quad (z_\delta z_\varepsilon)^{\delta\varepsilon} = (z_\delta z_\varepsilon)^{\varkappa\lambda+\varrho} = (z_\delta z_\varepsilon)^{\varkappa\lambda}.(z_\delta z_\varepsilon)^\varrho = (\mathfrak{G}p+1)^\varkappa(z_\delta z_\varepsilon)^\varrho \ (58.)$$
$$= \mathfrak{G}p+(z_\delta z_\varepsilon)^\varrho,$$

und da die niedrigere Potenz ϱ als λ von $z_\delta z_\varepsilon$ *nicht* $\mathfrak{G}p+1$ ist, so wäre nach (67.) *nicht* $(z_\delta z_\varepsilon)^{\delta\varepsilon} = \mathfrak{G}p+1$. Da dies der Gleichung (63.) widerspricht, so kann in (67. und 66.) ϱ nur Null sein; mithin mufs λ in $\delta\varepsilon$ *aufgehen* und folglich in (66.)

$$68.\quad \delta\varepsilon = \varkappa\lambda$$

sein.

d. Nun lassen *nur* die δ, 2δ, 3δ, ... $\varepsilon\delta$ten Potenzen von z_δ, und *nur* die ε, 2ε, 3ε, ... $\delta\varepsilon$ten Potenzen von z_ε zu p den Rest 1; keine der Potenzen mit *zwischenliegenden* Exponenten. Daraus folgt, dafs für kein Vielfaches, z. B. $\sigma\delta$, von δ, wenn $\sigma < \varepsilon$ ist, für welches nach (61.)

$$69.\quad z_\delta^{\sigma\delta} = \mathfrak{G}p+1$$

ist, *zugleich* in

$$70.\quad z_\varepsilon^{\sigma\delta} = \mathfrak{G}p+e$$

$e=1$ sein kann, sobald δ und ε zu einander *theilerfremd* sind. Denn da

z_ε *nur* mit Exponenten, die Vielfache von ε sind, wie $\tau\varepsilon$, $z^{\tau\varepsilon} = \mathfrak{S}p+1$ sein kann, so müfste $\sigma\delta = \tau\varepsilon$ sein können; was nur dann der Fall ist, wenn $\sigma = \varepsilon$ und $\tau = \delta$ ist, indem kein Theiler > 1 von ε in δ und kein Theiler > 1 von δ in ε aufgeht, folglich ε *ganz* in σ und τ *ganz* in δ aufgehen mufs.

Es ist also auch, vermöge (69. und 70.), in

$$71. \quad z_\delta^{\sigma\delta} z_\varepsilon^{\sigma\delta} = (z_\delta z_\varepsilon)^{\sigma\delta} = \mathfrak{S}p+e$$

für *kein* $\sigma < \varepsilon$ und auch nicht für ein in ε *aufgehendes* σ, $e = 1$.

e. Auf gleiche Weise folgt, dafs für kein $\sigma < \delta$, auch nicht für ein in δ *aufgehendes* σ, in

$$72. \quad z_\delta^{\sigma\varepsilon} z_\varepsilon^{\sigma\varepsilon} = (z_\delta z_\varepsilon)^{\sigma\varepsilon} = \mathfrak{S}p+e$$

$e = 1$ sein kann.

f. Es kann aber immer $\sigma\delta$ oder $\sigma\varepsilon$ ein *Vielfaches von* λ sein, sobald in (68.) $x > 1$ ist. Denn vermöge $x\lambda = \delta\varepsilon$ (68.) mufs x, oder irgend ein Theiler μ von x, in δ oder in ε aufgehen: also ist immer, wenn man $x = \mu\nu$ setzt,

$$73. \quad \nu\lambda = \frac{\delta}{\mu}\varepsilon \quad \text{oder} \quad = \delta . \frac{\varepsilon}{\mu},$$

wo, nächst ν, $\frac{\delta}{\mu}$ oder $\frac{\varepsilon}{\mu}$ eine *ganze* Zahl ist, die durch σ bezeichnet werden kann. Wäre x eine Stammzahl oder ohne Theiler, so wäre $\nu = 1$ und $\frac{\delta}{\mu} = \sigma$, oder $\frac{\varepsilon}{\mu} = \sigma$, gleich $\frac{\delta}{x}$ oder $\frac{\varepsilon}{x}$.

g. Nun giebt (65.)

$$74. \quad (z_\delta z_\varepsilon)^{\nu\lambda} = (z_\delta z_\varepsilon)^{\sigma\delta} = \mathfrak{S}p+1 \text{ oder}$$
$$75. \quad (z_\delta z_\varepsilon)^{\nu\lambda} = (z_\delta z_\varepsilon)^{\sigma\varepsilon} = \mathfrak{S}p+1.$$

Diese Gleichungen widersprechen denen (71. und 72.): also kann in (68.) x nicht > 1 sein. Wenn aber in (71. und 72.) $\sigma = \varepsilon$ oder $= \delta$ ist, so giebt (71. und 72.)

$$76. \quad (z_\delta z_\varepsilon)^{\delta\varepsilon} = \mathfrak{S}p+1 \text{ (64.)}.$$

Dies ist (74. und 75.) gemäfs; wo dann in (73.) $\sigma = \delta$ oder $= \varepsilon$, folglich $\mu = 1$, $\nu = 1$ und $\lambda = \delta\varepsilon$ ist.

Also kann *keine niedrigere* Potenz λ, als $\delta\varepsilon$ selbst, von $z_\delta z_\varepsilon$ zu p den Rest 1 geben; und folglich ist in (74.) das Product $z_\delta z_\varepsilon$ und mithin auch vermöge (7.) r, sobald $r > 1$, *nothwendig* eine δste Stammwurzel aus 1 zu p, wenn δ und ε zu einander *theilerfremd* sind; gemäfs (IX.).

Bew. von X. *S. a.* Wenn z_δ eine δte Stammwurzel aus 1 zu p ist und man setzt, wie in (8.),

$$77. \quad z_\delta^x = \mathfrak{S}p + r,$$

so ist, zufolge der Eigenschaft der *Stammwurzeln* für $x = 1, 2, 3, 4, \ldots \delta - 1$, r *nicht gleich* 1; erst für $x = \delta$ ist $r = 1$.

b. Ist nun x eine Zahl, von welcher die λte Potenz zu p die δte Stammwurzel z_δ *zum Rest* läfst, so dafs, wie in (9.),

$$78. \quad x^\lambda = \mathfrak{S}p + z_\delta$$

ist, so giebt (77.), wenn man darin aus (78.) $z_\delta = x^\lambda - \mathfrak{S}p$ setzt,

$$79. \quad x^{x\lambda} = \mathfrak{S}p + r = z_\delta^x,$$

und folglich ist, vermöge (*a.*), für die Exponenten λ, 2λ, 3λ, ... $(\delta - 1)\lambda$ von x in (79.) r *nicht gleich* 1.

c. Nun giebt (79.), für eine beliebige Zahl $\mu > 0 < \lambda$,

$$80. \quad x^{x\lambda + \mu} = \mathfrak{S}p + r x^\mu = z_\delta^x x^\mu.$$

Käme nun unter den verschiedenen Werthen von r in (77.) irgend ein Rest

$$81. \quad r = x^{\lambda - \mu} - \mathfrak{S}p$$

vor, so wäre in (80.)

$$82. \quad z_\delta^x x^\mu = \mathfrak{S}p + x^{\lambda - \mu} . x^\mu = \mathfrak{S}p + x^\lambda = \mathfrak{S}p + z_\delta \text{ (78.)}:$$

also müfste, da p nicht durch z_δ theilbar ist, $\mathfrak{S}$ mit z_δ *aufgehen*, und es wäre, wenn man (82.) mit z_δ dividirt,

$$83. \quad z_\delta^{x-1} x^\mu = \mathfrak{S}p + 1,$$

oder, da $z_\delta = x^{x\lambda} - \mathfrak{S}p$ ist (79.),

$$84. \quad x^{x\lambda - \lambda + \mu} = \mathfrak{S}p + 1.$$

d. Es ist aber der Exponent $x\lambda - (\lambda - \mu) < \delta\lambda$, weil $\mu < \lambda$ und in (77.) $x < \delta$ ist: also gäbe eine *niedrigere* Potenz von x als $x^{\delta\lambda}$ schon zu p den Rest 1, und folglich wäre dann x *keine* $\lambda\delta$te Stammwurzel aus 1 zu p.

e. Ist dagegen unter den Resten r in (77.) keiner weder $= x^1 - \mathfrak{S}p$, noch $= x^2 - \mathfrak{S}p$, $= x^3 - \mathfrak{S}p$, ... $= x^{\lambda-1} - \mathfrak{S}p$, also auch nicht $= x^{\lambda-\mu} - \mathfrak{S}p$, so ist in (80.) $r x^\mu$ *nicht* $= x^\lambda = \mathfrak{S}p + z_\delta$; folglich findet die Gleichung (82.), und mithin diejenige (83.) *nicht* Statt, und folglich ist auch alsdann *keine* niedrigere Potenz von x als $x^{\lambda\delta}$ gleich $\mathfrak{S}p + 1$.

f. Ist $x = \delta$, so ist in (79.)

$$85. \quad x^{\lambda\delta} = z_\delta^\delta = \mathfrak{S}p + 1,$$

also

$$86. \quad r = 1$$

und folglich in (81.)

$$87. \quad \lambda - \mu = 0$$

und in (83.)

$$88. \quad x^{\lambda\delta} = \mathfrak{S}p + 1;$$

aber keine niedrigere Potenz von x als $x^{\lambda\delta}$ giebt $\mathfrak{S}p+1$. Mithin ist, wenn r weder $= x^1 - \mathfrak{S}p$, noch $= x^2 - \mathfrak{S}p$, noch $= x^3 - \mathfrak{S}p$, ... bis zu $x^{\lambda-1} - \mathfrak{S}p$ ist, x eine $\lambda\delta$te Stammwurzel aus 1 zu p; gemäfs (X.).

§. 67.

Lehrsatz.

I. *Wenn man für eine δte Stammwurzel* z_δ *aus* 1 *zu* p

1. $z_\delta^1, z_\delta^2, z_\delta^3, \dots z_\delta^{\delta-1}, z_\delta^\delta = \mathfrak{S}p + (r_1, r_2, r_3, \dots r_{\delta-1}, r_\delta)$

setzt, und es ist λ irgend ein Theiler von δ, so ist

2. $r_1^\lambda + r_2^\lambda + r_3^\lambda + r_4^\lambda + \dots + r_\delta^\lambda = \mathfrak{S}p;$

das heifst, die Summe der λten Potenzen der Reste r *in* (1.) *geht mit* p *auf.*

II. *Das Product der Reste* r *in* (1.), *mit* p *dividirt, läfst, wenn δ ungerade ist,* $+1$, *und wenn δ gerade ist,* -1 *zum Rest; das heifst, es ist*

3. $r_1 r_2 r_3 r_4 \dots r_\delta = \mathfrak{S}p + 1$, *wenn δ ungerade und*

4. $r_1 r_2 r_3 r_4 \dots r_\delta = \mathfrak{S}p - 1$, *wenn δ gerade ist.*

III. *Zu jeder δten Stammwurzel* z_δ ($\delta = 2$ *ausgenommen*) *giebt es eine zweite δte Stammwurzel* x_δ, *und nur eine, welche, mit jener multiplicirt und das Product durch* p *dividirt, den Rest* 1 *giebt, so dafs*

5. $z_\delta . x_\delta = \mathfrak{S}p + 1$

ist. Die Stammwurzeln sind also immer zusammengehörige Zahlen für 1 *zu* p.

IV. *Das Product aller δten Stammwurzeln, für jedes δ, das einzige $\delta = 2$ ausgenommen, für welches es nur die einzige Stammwurzel* $p-1$ *giebt, ist* $= \mathfrak{S}p + 1$.

Beispiele. (Aus Taf. I.) Zu I. Für die $\delta = 12$te Stammwurzel $z_\delta = 29$ aus 1 zu p ist die Summe der Reste zu den 1ten, 2ten, 3ten, ... δten Potenzen von $z = 29$,

6. $29+48+50+47+21+60+32+13+11+14+40+1 = 366 = 6.p$,

und geht also mit p auf.

Ein Theiler λ von δ ist z. B. 4, und die Summe der $\lambda = 4$ten Potenzen der Reste (6.) ist, wenn man die Zahlen r in (6.) in der *obersten* horizontalen Zeile der Tafel aufsucht und die zugehörigen Zahlen der *vierten* horizontalen Zeile nimmt,

7. $47+13+1+47+13+1+47+13+1+47+13+1 = 244 = 4.p$.

Diese Summe geht also ebenfalls mit p auf; gemäfs (I.).

Zu II. Das *Product* der Reste r in (6.) findet sich wie folgt: $29.48 = \mathfrak{S}p + 50$; $50.50 = -11.-11 = \mathfrak{S}p + 60 = \mathfrak{S}p - 1$; $-1.47 = \mathfrak{S}p - 47 = \mathfrak{S}p + 14$; $14.21 = \mathfrak{S}p + 50$; $50.60 = -11.-1 = \mathfrak{S}p + 11$; $11.32 = \mathfrak{S}p + 47$; $47.13 = \mathfrak{S}p + 1$; $1.11 = \mathfrak{S}p + 11$; $11.14 = \mathfrak{S}p + 32$; $32.40 = \mathfrak{S}p - 1$; $-1.+1 = \mathfrak{S}p - 1$: also ist für das *gerade* $\delta = 12$ das Product der Reste r gleich $\mathfrak{S}p - 1$; gemäfs (4.).

Für das *ungerade* $\delta = 5$ sind z. B. von der 5ten Stammwurzel $z_\delta = 20$ die Reste der 1ten, 2ten, 3ten, 4ten und 5ten Potenz, der Tafel gemäfs, $r = 20, 34, 9, 58$ und 1. Ihr Product ist $20.34 = \mathfrak{S}p + 9$; $9.9 = \mathfrak{S}p + 20$; $20.58 = \mathfrak{S}p + 1$; $1.1 = \mathfrak{S}p + 1$: also ist für das *ungerade* $\delta = 5$ das Product der Reste r gleich $\mathfrak{S}p + 1$; gemäfs (3.).

Zu III. Die $\delta =$ 10ten Stammwurzeln z. B. sind 3, 27, 41 und 52, und es ist $3.41 = 2.p + 1$ und $27.52 = 1404 = 23.p + 1$; gemäfs (III.).

Die $\delta =$ 15ten Stammwurzeln sind 12, 15, 16, 22, 25, 42, 56, 57 und es ist $12.56 = 672 = 11.p + 1$; $15.57 = 855 = 14.p + 1$; $16.42 = 672 = 11.p + 1$ und $22.25 = 550 = 9.p + 1$; gemäfs (III.).

Zu IV. Die $\delta =$ 5ten Stammwurzeln sind 9, 20, 34, 58. Ihr Product ist $9.20 = \mathfrak{S}p - 3$; $-3.34 = \mathfrak{S}p - 41 = \mathfrak{S}p + 20$; $20.58 = -41.-3 = 123 = \mathfrak{S}p + 1$; gemäfs (IV.).

Beweis von I. *A.* Nimmt man von (1.) die Summe der λten Potenzen, so ergiebt sich

$$8. \quad z_\delta^\lambda + z_\delta^{2\lambda} + z_\delta^{3\lambda} + z_\delta^{4\lambda} + \ldots + z_\delta^{\delta\lambda} = \mathfrak{S}p + r_1^\lambda + r_2^\lambda + r_3^\lambda + r_4^\lambda + \ldots + r_\delta^\lambda.$$

Aber es ist, vermöge der Eigenschaft der *Stammwurzeln*,

$$9. \quad z_\delta^\delta = \mathfrak{S}p + 1 \quad \text{und} \quad z_\delta^{\delta\lambda} = \mathfrak{S}p + 1,$$

also, da $z_\delta^\delta = \mathfrak{S}p + r_\delta$ sein soll,

$$10. \quad r_\delta = 1 \quad \text{und} \quad r_\delta^\lambda = 1.$$

Dies in (8.) gesetzt, giebt

$$11. \quad z_\delta^\lambda + z_\delta^{2\lambda} + z_\delta^{3\lambda} + z_\delta^{4\lambda} \ldots + z_\delta^{(\delta-1)\lambda} + \mathfrak{S}p + 1 = r_1^\lambda + r_2^\lambda + r_3^\lambda + r_4^\lambda \ldots + r_{\delta-1}^\lambda + 1.$$

B. Nun ist

$$12. \quad 1 + z_\delta^\lambda + z_\delta^{2\lambda} + z_\delta^{3\lambda} + \ldots + z_\delta^{(\delta-1)\lambda} = \frac{z_\delta^{\delta\lambda} - 1}{z_\delta - 1};$$

wie erhellet, wenn man diese Gleichung mit $z_\delta - 1$ multiplicirt.

Aus (9.) ist $z_\delta^\delta - 1 = \mathfrak{S}p$, also $\dfrac{z_\delta^{\lambda\delta} - 1}{z_\delta - 1} = \dfrac{\mathfrak{S}p}{z_\delta - 1}$ und es mufs, da p

nicht mit $z_\delta - 1$ aufgeht, $\mathfrak{S}$ mit $z_\delta - 1$ aufgehen und folglich

$$13.\quad \frac{z_\delta^{\lambda\delta}-1}{z_\delta-1} = \mathfrak{S}p$$

sein.

C. Dieses giebt in (12.)

$$14.\quad 1+z_\delta^{\lambda}+z_\delta^{2\lambda}+z_\delta^{3\lambda}+\ldots+z_\delta^{(\delta-1)\lambda} = \mathfrak{S}p$$

und in (11.) $\mathfrak{S}p+\mathfrak{S}p = r_1^\lambda+r_2^\lambda+r_3^\lambda+\ldots+r_{\delta-1}^\lambda+1$, oder, da $1=r_\delta^\lambda$ ist (10.),

$$15.\quad r_1^\lambda+r_2^\lambda+r_3^\lambda+r_4^\lambda+\ldots+r_{\delta-1}^\lambda+r_\delta^\lambda = \mathfrak{S}p;$$

wie (1.).

Bew. von II. *D.* Multiplicirt man die Gleichungen (1.) mit einander, so ergiebt sich

$$16.\quad z_\delta^{1+2+3+4+\ldots+\delta-1}.z_\delta^\delta = \mathfrak{S}p+r_1r_2r_3\ldots r_{\delta-1}r_\delta$$

oder, da $z_\delta^\delta = \mathfrak{S}p+1$ (9.) ist,

$$17.\quad z_\delta^{1+2+3+4+\ldots+\delta-1} = \mathfrak{S}p+r_1r_2r_3\ldots r_{\delta-1}r_\delta$$

oder

$$18.\quad z_\delta^{\frac{1}{2}\delta(\delta-1)} = \mathfrak{S}p+r_1r_2r_3\ldots r_{\delta-1}r_\delta.$$

a. Ist nun δ *ungerade*, also $\delta-1$ *gerade*, so giebt (18.), wegen $z_\delta^\delta = \mathfrak{S}p+1$ (9.), $(\mathfrak{S}p+1)^{\frac{1}{2}(\delta-1)} = \mathfrak{S}p+r_1r_2r_3\ldots r_\delta$ oder

$$19.\quad r_1r_2r_3\ldots r_\delta = \mathfrak{S}p+1;$$

gemäfs (3.).

b. Ist δ *gerade*, also $\delta-1$ *ungerade*, so ist $z_\delta^{\frac{1}{2}\delta} = \mathfrak{S}p-1$ (§. 66. I.); also giebt dann (18.) $(\mathfrak{S}p-1)^{\delta-1} = \mathfrak{S}p+r_1r_2r_3\ldots r_\delta$ und, da $\delta-1$ ungerade ist,

$$20.\quad r_1r_2r_3\ldots r_\delta = \mathfrak{S}p-1;$$

gemäfs (4.).

Bew. von III. *E.* Gemäfs (§. 47. I.) giebt es zu jeder der Zahlen

$$21.\quad z = 2, 3, 4, 5, \ldots p-1$$

eine zweite, von z_1 *verschiedene* Zahl z_2 aus derselben Reihe, und *nur eine*, für welche

$$22.\quad z_1z_2 = \mathfrak{S}p+1$$

ist.

F. (22.) giebt für *jeden* beliebigen Exponenten x

$$23.\quad z_1^x z_2^x = \mathfrak{S}p+1.$$

Ist nun z_1 eine δte Stammwurzel aus 1 zu p, so ist vermöge ihrer Eigenschaften, wenn man

$$24.\quad z_1^x = \mathfrak{S}p+e$$

setzt, e für $x=1,2,3,4,\ldots\delta-1$ *nicht* $=1$, für $x=\delta$ aber *nothwendig* $=1$.

G. Setzt man andrerseits

$$25. \quad z_2^x = \mathfrak{G}p + \varepsilon,$$

so ist aus (24. und 25.)

$$26. \quad z_1^x z_2^x = (\mathfrak{G}p + e)(\mathfrak{G}p + \varepsilon) = \mathfrak{G}p + e\varepsilon$$

und vermöge (23.)

$$27. \quad e\varepsilon = \mathfrak{G}p + 1.$$

H. Da nun nach (*F.*) e für $x = 1, 2, 3, 4, \ldots \delta - 1$ *nicht* $= 1$ ist, so kann auch gemäfs (27.) ε für $x = 1, 2, 3, 4, \ldots \delta - 1$ *nicht* $= 1$ sein; denn wäre $\varepsilon = 1$ für eines dieser x, so wäre $e\varepsilon$ nicht $= \mathfrak{G}p + 1$, wie es sein soll, sondern $= \mathfrak{G}p + e$.

Da ferner nach (*F.*) für $x = \delta$, e nothwendig $= 1$ ist, so ist auch vermöge (27.) für $x = \delta$, ε nothwendig $= 1$; denn wäre ε nicht $= 1$, so wäre nicht $e\varepsilon = \mathfrak{G}p + 1$, wie es sein soll, sondern $= \mathfrak{G}p + \varepsilon$.

I. Es mufs also in (25.) für $x = 1, 2, 3, 4, \ldots \delta - 1$, ε *nicht* $= 1$ und für $x = \delta$, ε *gleich* 1 sein, und deshalb ist z_2 nothwendig eine δte Stammwurzel, wenn z_1 eine solche ist. Mithin giebt es nothwendig zu jeder δten Stammwurzel $z_1 = z_\delta$ eine zweite $z_2 = x_\delta$, welche, mit jener multiplicirt und das Product durch p dividirt, den Rest 1 giebt.

K. Und zwar giebt es *nur eine* solche: denn gäbe es eine zweite z_3, für welche

$$28. \quad z_1 z_3 = \mathfrak{G}p + 1$$

wäre, so wäre

$$29. \quad \text{aus (22.)} \quad z_1 z_2 z_3 = \mathfrak{G}p + z_3$$

$$30. \quad \text{und aus (28.)} \quad z_1 z_2 z_3 = \mathfrak{G}p + z_2.$$

Da (29.) und (30.) sich widersprechen, wenn nicht $z_2 = z_3$ ist, so kann es keine zweite zu z_1 gehörige Stammwurzel geben.

Dieses zusammen ist was (III.) behauptet und es folgt, dafs die Stammwurzeln *zusammengehörige Zahlen* für 1 zu p sind.

Bew. von IV. *L.* Wenn z_δ eine der δten Stammwurzeln aus 1 zu p ist und man setzt

$$31. \quad z_\delta^x = \mathfrak{G}p + r_x,$$

so sind nach (§. 60. II.) die Reste r für diejenigen Exponenten x, welche zu δ *theilerfremd* sind, *alle die δten Stammwurzeln* z_δ selbst.

Bezeichnet man also die zu δ *theilerfremden* x durch x_1, x_2, x_3, ... und die in (31.) zugehörigen *Reste* durch r_1, r_2, r_3, ..., so dafs für *irgend eine* der δten Stammwurzeln z_δ

$$32. \quad \begin{cases} z_\delta^{x_1} = \mathfrak{G}p + r_1, \\ z_\delta^{x_2} = \mathfrak{G}p + r_2, \\ z_\delta^{x_3} = \mathfrak{G}p + r_3, \\ \ldots\ldots\ldots\ldots \end{cases}$$

ist, so sind die r in (32.) alle die δten Stammwurzeln z_δ selbst.

M. Multiplicirt man nun die Gleichungen (32.) mit einander, so ergiebt sich

$$33. \quad z_\delta^{x_1+x_2+x_3+x_4+\ldots} = \mathfrak{G}p + r_1 r_2 r_3 r_4 \ldots.$$

Nun *geht* aber nach (§. 65. II.) die Summe $x_1 + x_2 + x_3 + x_4 \ldots$, aller zu der Zahl δ theilerfremden Zahlen, $\delta = 2$ ausgenommen, mit δ *auf*, also giebt (33.)

$$34. \quad z_\delta^{\mathfrak{G}\delta} = \mathfrak{G}p + r_1 r_2 r_3 r_4 \ldots,$$

und da vermöge der Eigenschaft der Stammwurzeln $z_\delta^\delta = \mathfrak{G}p + 1$, also auch $z_\delta^{\mathfrak{G}\delta} = \mathfrak{G}p + 1$ ist, so giebt (34.)

$$35. \quad r_1 r_2 r_3 r_4 \ldots = \mathfrak{G}p + 1;$$

das heifst: das Product aller δten Stammwurzeln r_1, r_2, r_3, r_4, ... aus 1 zu p ist $= \mathfrak{G}p + 1$. $\delta = 2$ ist ausgenommen, für welches δ es *nur die eine* Stammwurzel $p - 1$ giebt.

Anm. *N.* Immer, wenn bewiesen werden soll, dafs z z. B. eine δte *Stammwurzel* aus 1 zu der Stammzahl p sei, ist nicht zu übersehen, dafs deshalb, weil etwa sich findet, die δte Potenz von z durch p dividirt lasse den Rest 1, das heifst, die Gleichung $z^\delta = \mathfrak{G}p + 1$ werde erfüllt, z noch keineswegs *nothwendig* eine δte Stammwurzel aus 1 zu p sei. Es mufs vielmehr immer noch besonders bewiesen werden, dafs keine *niedrigere* als die δte Potenz von z, durch p dividirt, den Rest 1 läfst; denn dies ist die *zweite* Bedingung für *Stammwurzeln.*

§. 68.

Lehrsatz.

I. -3 *ist Quadratrest zu allen Stammzahlen* $\mathrm{p} = 6\mathrm{n} + 1$ *und Nichtquadratrest zu allen Stammzahlen* $\mathrm{p} = 6\mathrm{n} - 1$.

II. $+3$ *ist Quadratrest zu allen Stammzahlen* $\mathrm{p} = 12\mathrm{n} + 1$ *und* $12\mathrm{n} - 1$ *und Nichtquadratrest zu allen Stammzahlen* $\mathrm{p} = 12\mathrm{n} + 5$ *und* $12\mathrm{n} - 5$.

III. *Setzt man für die Stammzahlen* $\mathrm{p} = 6\mathrm{n} + 1$

$$1. \quad \mathrm{z}^2 = \mathfrak{G}\mathrm{p} - 3,$$

wo z *die beiden Werthe* z *und* p — z *hat, so sind die beiden **dritten Stammwurzeln*** x_3 *aus* 1 *zu* p:

2. $x_3 = \frac{1}{2}(z-1)$ *oder* $\frac{1}{2}(p-z-1)$ *und*

3. $x_3 = p-\frac{1}{2}(z+1)$ *oder* $\frac{1}{2}(p+z-1)$.

IV. *Die beiden **sechsten Stammwurzeln*** x_6 *aus* 1 *zu* p *sind um* 1 ***gröfser**, also*

4. $x_6 = \frac{1}{2}(z+1)$ *oder* $\frac{1}{2}(p-z+1)$ *und*

5. $x_6 = p-\frac{1}{2}(z-1)$ *oder* $\frac{1}{2}(p+z+1)$.

Beispiele. Zu I. und III. Wie aus der Tafel im 9ten Bande dieses Journals S. 36 — 53 zu ersehen, ist

6.
1. -3 *Quadratrest* zu $p =$ 5 7 13 19 31 37 43 61 67 73 79 97 .... $= 6n+1$,
2. und *Nichtquadratrest* zu $p =$ 11 17 23 29 41 47 53 59 71 83 89 101 .... $= 6n-1$,
3. $+3$ ist *Quadratrest* zu $p =$ 11 13 23 37 47 59 61 71 73 83 97 .... $= 12n \pm 1$,
4. und *Nichtquadratrest* zu $p =$ 5 7 17 19 29 31 41 43 53 67 79 89 101 .... $= 12n \pm 5$.

Zu III. 1. Nach Taf. I. ist $27^2 = \mathfrak{S}p+58 = \mathfrak{S}p-3$ und $34^2 = \mathfrak{S}p+58 = \mathfrak{S}p-3$, also hat für $p = 61 = 6n+1$, z in (1.) die beiden Werthe 27 und 34. $z = 27$ giebt nach (2. und 3.) $x_3 = \frac{1}{2}(27-1) = 13$ und $x_3 = 61-\frac{1}{2}(27+1) = 61-14 = 47$; $z = 34$ giebt ebenfalls $x_3 = \frac{1}{2}(61-34-1) = 13$ und $x_3 = \frac{1}{2}(61+34-1) = 47$, und 13 und 47 sind, wie die Tafel zeigt, die beiden *dritten* Stammwurzeln aus 1 zu p. Die beiden *sechsten* Stammwurzeln aus 1 zu p, der Tafel nach 14 und 48, sind *um* 1 *gröfser*.

2. Für $p = 43$ ist $13^2 = \mathfrak{S}p+40 = \mathfrak{S}p-4$ und $30^2 = \mathfrak{S}p+40 = \mathfrak{S}p-3$; also hat hier z in (1.) die beiden Werthe 13 und 30. $z = 13$ giebt nach (2. und 3.) $x_3 = \frac{1}{2}(13-1) = 6$ und $x_3 = 43-\frac{1}{2}(13+1) = 43-7 = 36$, und $z = 30$ giebt $x_3 = \frac{1}{2}(43-30-1) = 6$ und $x_3 = \frac{1}{2}(43+30-1) = 36$, und 6 und 36 sind die beiden *dritten* Stammwurzeln aus 1 zu p. Die beiden *sechsten* Stammwurzeln aus 1 zu p sind 7 und 37, also um 1 gröfser.

Beweis. *A.* Für die dritten *Stammwurzeln* aus 1 zu p ist

7. $x^3 = \mathfrak{S}p+1$.

Von den *drei* ganzzahligen Werthen >0 und $<p$, welche x für diese Gleichung nach (§. 54.) haben *kann* und von welchen $x = 1$ einer ist, sind nothwendig die beiden andern, >1, *dritte Stammwurzeln* aus 1 zu p, weil die *zwei* Zahlen 1 und 2 mit 3 keinen Theiler >1 gemein haben und also nach (§ 63. I.) *zwei* Stammwurzeln, folglich *zwei* Werthe von $x>1$ Statt finden müssen, die der Gleichung (7.) genugthun, und die also die *beiden andern* ganzzahligen Wurzeln der Gleichung (7.) sind, welche es *aufser* $x = 1$ geben kann und hier also geben *mufs*.

B. Die beiden Wurzeln, >1, von der Gleichung (7.) sind diejenigen der Gleichung

$$8. \quad x^2+x+1 = \mathfrak{G}p;$$

denn (7.) giebt

$$9. \quad x^3-1 = (x-1)(x^2+x+1) = \mathfrak{G}p,$$

und dieser Gleichung wird zunächst durch $x=1$ und dann durch die beiden Werthe, welche x in (8.) haben kann, entsprochen.

C. Löset man nun die quadratische Gleichung (8.) auf die gewöhnliche Weise auf, so ergiebt sich $x=-\frac{1}{2}\pm\sqrt{(\frac{1}{4}-1+\mathfrak{G}p)}$ oder

$$10. \quad x = \frac{-1\pm\sqrt{(\mathfrak{G}p-3)}}{2}.$$

Diese beiden Werthe von x, welche (10.) ausdrückt, sind also die beiden *dritten Stammwurzeln* >1 aus 1 zu p.

D. Geht nun $p-1$ mit 3 auf, und mithin, da $p-1$ *immer gerade* ist und folglich *zugleich* mit 2 aufgeht, mit 6 (§. 26.), so dafs p von der Form $p=6n+1$ ist, so giebt es *nothwendig* ganzzahlige dritte Stammwurzeln aus 1 zu p; denn es giebt deren nach (§. 58. I.) für *jeden* Theiler δ von $p-1$, also hier auch für $\delta=3$. Daraus folgt, dafs der Ausdruck in (10.) von x *ganze Zahlen* geben *mufs*.

E. Dieses aber ist nicht anders möglich, als wenn $\mathfrak{G}p-3$ ein *Quadrat* und folglich -3 ein *Quadratrest* zu p ist. Denn wäre $\mathfrak{G}p-3$ *nicht* ein Quadrat, für kein $\mathfrak{G}$, so wäre $\sqrt{\mathfrak{G}p-3}$ eine *irrationale* und folglich x keine *ganze* Zahl. Also *mufs* nothwendig nach (1.)

$$11. \quad z^2 = \mathfrak{G}p-3$$

und also in (10.)

$$12. \quad x = \frac{-1\pm z}{2}$$

sein.

F. Mehr, als dafs $\mathfrak{G}p-3$ ein Quadrat z sei, ist aber auch in (10.) nicht nöthig, um die beiden Werthe von x zu *ganzen* Zahlen zu machen. Denn der Gleichung (11.) thut auch ebensowohl $p-z$ als z ein Genüge; also ist auch in (10.), ebensowohl wie in (12.), $x=\frac{-1\pm z}{2}$ ist, auch

$$13. \quad x = \frac{-1\pm(p-z)}{2}.$$

Ist nun z *ungerade*, so sind in (12.) $z-1$ und $-z-1=-(z+1)$ beide *gerade*, und folglich sind x zwei ganze Zahlen. Ist z *gerade*, so ist $p-z$ *ungerade*, und es folgt auf dieselbe Weise, dafs dann die x in (13.)

zwei ganze Zahlen sind. Es gilt (12.) für den *ungeraden*, (13.) für den *geraden* Werth von z; und so geben denn auch die beiden Gleichungen (12. und 13.) nicht etwa *vier* verschiedene Werthe von x, sondern nur *dieselben zwei* Werthe. Denn ist in (12.) z *ungerade*, so mufs man für (13.) den *geraden* Werth von z nehmen, welcher $p-z$ ist, und dadurch reducirt sich (13.) auf $x=\frac{-1\pm(p-(p-z))}{2}=\frac{-1\pm z}{2}$, welches *Dasselbe* wie (12.) ist. Ist in (13.) z *gerade*, so mufs man für (12.) den andern, *ungeraden* Werth von z setzen, welcher $p-z$ ist, damit *so* alle verschiedenen Werthe in Rechnung kommen; und dadurch reducirt sich (12.) auf $x=\frac{-1\pm(p-z)}{2}$; welches Dasselbe wie (13.) ist.

Bis hierher folgt also, dafs für Stammzahlen $p=6n+1$, -3 nothwendig *Quadratrest* sein mufs und dafs dann

$$14. \quad x_3 = \tfrac{1}{2}(z-1) \quad \text{oder} \quad \tfrac{1}{2}(p-z-1)$$

und $x_3 = -\frac{1}{2}(z+1)$ oder $-\frac{1}{2}(p-z+1)$, oder, was dasselbe ist,

$$15. \quad x_3 = p-\tfrac{1}{2}(z+1) \quad \text{oder} \quad p-\tfrac{1}{2}(p-z+1) = \tfrac{1}{2}(p+z-1)$$

die beiden dritten Stammwurzeln aus 1 zu p sind; wie es (I.) und (III.) behauptet.

G. Ferner sind die 6ten Stammwurzeln x_6, aus 1 zu p, da 3 eine *Stammzahl* ist, nach (§. 66. VI.) $=p-z$. Man findet sie also, wenn man die x_3 (2. und 3.) von p abzieht. Dieses giebt die Ausdrücke (IV. 4. und 5.) von x_6. Die sechsten Stammwurzeln aus 1 zu p sind, wie (4. und 5.) zeigen, um 1 gröfser als die dritten.

H. Ist p von der Form $6n-1$, so geht $p-1=6n-2$ *nicht* mit 3 auf, und folglich giebt es für $p=6n-1$ *keine* dritten Stammwurzeln aus 1 zu p. Es gäbe aber dergleichen vermöge (10.), wenn -3 auch für die Stammzahlen $p=6n-1$ *Quadratrest* wäre. Also kann -3 für solche Stammzahlen *kein* Quadratrest sein. Und da nun *jede* Zahl entweder Quadratrest oder Nichtquadratrest ist, so ist -3 für alle Stammzahlen $p=6n-1$ nothwendig *Nichtquadratrest;* gemäfs (I.).

I. a. Nach (§. 50. I.) sind für Stammzahlen $p=4n+1$, für welche also $p-1$ mit 4 aufgeht, die *zeichenfreien* Werthe der positiven und der negativen *Quadratreste dieselben.* Nun ist -3 Quadratrest zu den Stammzahlen $p=6n+1$ (I.), für welche $p-1$ mit 6 aufgeht. Geht also $p-1$ mit 4 und mit 6 *zugleich* auf, so ist auch $+3$ *Quadratrest* zu p. Jenes ist der Fall für $p=12n+1$; also ist zu den Stammzahlen $p=12n+1$, $+3$ *Quadratrest;* gemäfs (II.).

b. Eben so sind nach (§. 50. I.) für Stammzahlen $p = 4n + 1$, für welche also $p - 1$ mit 4 aufgeht, die *zeichenfreien* Werthe der positiven und der negativen *Nichtquadratreste* dieselben. Nun ist -3 Nichtquadratrest zu den Stammzahlen $p = 6n - 1$ (I.), für welche $p + 1$ mit 6 aufgeht. Geht also $p - 1$ mit 4 und zugleich $p + 1$ mit 6 auf, so ist auch $+3$ *Nichtquadratrest* zu p. Jenes ist der Fall für $p = 12n + 5$: also ist zu den Stammzahlen $p = 12n + 5$, $+3$ *Nichtquadratrest;* gemäfs (II.).

c. Nach (§. 50. II.) sind für die Stammzahlen $p = 4n - 1$, für welche $p + 1$ mit 4 aufgeht, die zeichenfreien Werthe der negativen *Nichtquadratreste* die positiven *Quadratreste.* Nun ist nach (I.) -3 *Nichtquadratrest* zu den Stammzahlen $p = 6n - 1$, für welche $p + 1$ mit 6 aufgeht. Geht also $p - 1$ mit 4 und mit 6 *zugleich* auf, so ist $+3$ *Quadratrest* zu p. Jenes ist der Fall für $p = 12n - 1$: also ist zu den Stammzahlen $p = 12n - 1$, $+3$ *Quadratrest;* gemäfs (II.).

d. Endlich sind nach (§. 50. II.) für die Stammzahlen $p = 4n - 1$, für welche $p + 1$ mit 4 aufgeht, die zeichenfreien Werthe der negativen *Quadratreste* die positiven *Nichtquadratreste.* Nun ist nach (I.) -3 *Quadratrest* zu den Stammzahlen $p = 6n + 1$, für welche also $p - 1$ mit 6 aufgeht. Geht also $p + 1$ mit 4 und *zugleich* $p - 1$ mit 6 auf, so ist $+3$ *Nichtquadratrest* zu p. Jenes ist der Fall für $p = 12n - 5$: also ist zu den Stammzahlen $p = 12n - 5$, $+3$ *Nichtquadratrest;* gemäfs (II.).

Zweiter Beweis von I. und II. *K.* Nach dem *Gegenseitigkeitsgesetze für Quadratreste* (§. 49. II.) sind zwei Stammzahlen p und q zu einander *zugleich* positiver Quadratrest oder positiver Nichtquadratrest, wenn p und q nicht beide von der Form $4n - 1$ sind; und zugleich positiver Quadratrest und positiver Nichtquadratrest, oder umgekehrt, wenn *beide* von der Form $4n - 1$ sind. Nach (49. I.) aber ist, wenn z. B. p *Quadratrest* zu q ist, also in (§. 49. 1.) die Stelle von r einnimmt,

$$16. \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q + 1,$$

und wenn p *Nichtquadratrest* zu q ist, also in (§. 49. 2.) die Stelle von ϱ einnimmt,

$$17. \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q - 1.$$

Also im Fall p und q *nicht beide* von der Form $4n - 1$ sind, ist nach dem Gegenseitigkeitsgesetz:

$$18. \quad \textit{Zugleich} \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q + 1 \quad \text{und} \quad q^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1 \quad \text{und}$$

$$19. \quad \textit{Zugleich} \quad p^{\frac{1}{2}(q-1)} = \mathfrak{G}q - 1 \quad \text{und} \quad q^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1.$$

Sind p und q *beide* von der Form $4n-1$, so ist

20. *Zugleich* $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q+1$ und $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$ und

21. *Zugleich* $p^{\frac{1}{2}(q-1)} = \mathfrak{G}q-1$ und $q^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$.

L. Nun ist die Zahl 3, von welcher man wissen will, zu welchen Stammzahlen p sie Quadratrest oder Nichtquadratrest sei, ebenfalls eine *Stammzahl:* es gilt also von ihr, p gegenüber, das Gegenseitigkeitsgesetz und man kann sie *statt* q setzen. Dieses giebt

a. In (18.)

$$22. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3+1:$$

also, wenn zunächst p von der Form $3\mathfrak{G}+1$ oder $3n+1$ ist, so ist nach (18.) *zugleich* $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, und folglich ist nach (§. 49. I.) $+3$ *Quadratrest* zu p. Aber es kommt für (18.) zugleich darauf an, dafs p und q *nicht beide* von der Form $4n-1$ sind. Hier ist $3=q$ von der Form $4n-1$, also gilt (18.) nur, wenn p von der Form $4n+1$ ist. Mithin mufs p *zugleich* von der Form $3n+1$ und von der Form $4n+1$ sein, folglich von der Form $12n+1$, wenn $+3$ *Quadratrest* zu p sein soll.

b. Setzt man in (19.) 3 statt q, so ergiebt sich

$$23. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3-1:$$

also, wenn zunächst p von der Form $3\mathfrak{G}-1$ oder $3n-1$ ist, so ist nach (19.) zugleich $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$ und folglich $+3$ nach (§. 49. 2.) *Nichtquadratrest* zu p. Aber es mufs wieder, wie vorhin, p *zugleich* von der Form $4n+1$ sein, weil $q=3$ von der Form $4n-1$ ist und, wenn (19.) Statt finden soll, p und q *nicht beide* von der Form $4n-1$ sein dürfen. Also mufs p von der Form $3n-1$ und zugleich von der Form $4n+1$, also von der Form $12n+5$ sein, wenn $+3$ *Nichtquadratrest* zu p sein soll; denn zu $12n+5$, 1 addirt, geht mit 3, und 1 davon abgezogen, geht mit 4 auf.

c. Setzt man 3 statt q in (20.), so ergiebt sich

$$24. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3+1,$$

also, wenn zunächst p von der Form $3n+1$ ist, so ist nach (20.) *zugleich* $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1$, also nach (§. 49. 2.) $+3$ *Nichtquadratrest* zu p; aber nur insofern p zugleich, eben wie $q=3$, von der Form $4n-1$ ist; der Bedingung für (20.) gemäfs. Wenn also p von der Form $3n+1$ und $4n-1$ *zugleich* ist, so ist $+3$ *Nichtquadratrest* zu p. Dieses giebt die Form $12n-5$; denn 1 davon abgezogen geht mit 3, und 1 dazu addirt, mit 4 auf.

d. Setzt man endlich 3 statt q in (21.), so ergiebt sich

$$25. \quad p^{\frac{1}{2}(3-1)} = p = \mathfrak{G}.3-1,$$

also, wenn zunächst p von der Form $3n-1$ ist, so ist nach (21.) *zugleich* $3^{\frac{1}{2}(p-1)} = \mathfrak{G}p+1$, also nach (§. 49. 1.) $+3$ *Quadratrest* zu p; aber nur insofern p zugleich, eben wie $q=3$, von der Form $4n-1$ ist; der Bedingung für (21.) gemäfs. Wenn also p von der Form $3n-1$ und $4n-1$ *zugleich* ist, so ist $+3$ *Quadratrest* zu p. Dieses giebt die Form $12n-1$; denn, 1 dazu addirt, geht mit 3 und mit 4 auf.

e. *Zusammen* also ist nach (*a.* und *d.*) und nach (*b.* und *c.*)

26. $+3$ *Quadratrest* zu p, wenn p von der Form $12n+1$ oder $12n-1$ ist und
27. $+3$ *Nichtquadratrest* zu p, wenn p von der Form $12n+5$ oder $12n-5$ ist;
gemäfs (II.).

M. Zu welchen Stammzahlen p, -3 Quadratrest oder Nichtquadratrest sei, kann man auf den Grund dessen, was so eben für $+3$ gefunden worden ist, aus dem Lehrsatze (§. 50.) abnehmen.

a. Nemlich, nach (§. 50. I.) sind die *zeichenfreien* Werthe der positiven und negativen echten Quadratreste und Nichtquadratreste für alle Stammzahlen $p=4n+1$ *dieselben*. Von der Form $4n+1$ sind in (26. und 27.) die Formen $12n+1$ und $12n+5$. Also ist zu $p=12n+1$, eben wie $+3$, auch -3 *Quadratrest*, und zu $p=12n+5$, eben wie $+3$, auch -3 *Nichtquadratrest.*

b. Nach (§. 50. II.) geben für alle Stammzahlen $p=4n-1$ die positiven Quadratreste die zeichenfreien Werthe der negativen Nichtquadratreste und die positiven Nichtquadratreste die zeichenfreien Werthe der negativen Quadratreste. Von der Form $4n-1$ sind in (26. und 27.) die Formen $12n-1$ und $12n-5$. Also ist zu $p=12n-1$, -3 *Nichtquadratrest* und zu $p=12n-5$, -3 *Quadratrest.*

c. Zusammen also ist zufolge (*a.* und *b.*) -3 *Quadratrest* zu $p=12n+1$ und zu $p=12n-5$, und *Nichtquadratrest* zu $p=12n+5$ und $p=12n-1$. Die Form $6n+1$ drückt, wenn man $2n$ und $2n-1$ statt n setzt, $12n+1$ und $6(2n-1)+1=12n-1$ *zugleich* aus. Eben so drückt die Form $6n-1$, wenn man $2n+1$ und $2n$ statt n setzt, $6(2n+1)-1 = 12n-5$ und $12n-1$ *zugleich* aus. Also ist, kürzer:

28. -3 *Quadratrest* zu p, wenn p von der Form $6n+1$ ist und
29. -3 *Nichtquadratrest* zu p, wenn p die Form $6n-1$ hat;
gemäfs (I.).

Man kann indessen die Resultate für -3 auch wie folgt direct aus dem Gegenseitigkeitsgesetz entnehmen.

N. Da $q=3$ von der Form $4n-3$ ist, so gelten (18. und 19.) *nur* für $p=4n+1$, und (20. und 21.) *nur* für $p=4n-1$.

a. Ist nun $p=4n+1$, so ist $\frac{1}{2}(p-1)=\frac{1}{2}.4n=2n$ eine *gerade* Zahl, also ist $(-3)^{\frac{1}{2}(p-1)}=(+3)^{\frac{1}{2}(p-1)}$. Für die p, welche *die Form* $4n+1$ *haben*, kann man also -3 statt $+3$ setzen: also zu allen den $p=4n+1$, zu welchen $+3$ Quadratrest oder Nichtquadratrest ist, ist es auch -3. In (*L. a.*) ist $p=4n+1$, und $+3$ ist *Quadratrest* zu $p=12n+1$, also ist auch -3 *Quadratrest* zu $p=12n+1$.

In (*L. b.*) ist $p=4n+1$ und $+3$ *Nichtquadratrest* zu $p=12n+5$, also ist auch -3 Nichtquadratrest zu $p=12n+5$.

b. Ist $p=4n-1$, so ist $\frac{1}{2}(p-1)=\frac{1}{2}(4n-2)=2n-1$ eine *ungerade* Zahl, also ist $(-3)^{\frac{1}{2}(p-1)}=-(+3)^{\frac{1}{2}(p-1)}$, und folglich ist, wenn $(+3)^{\frac{1}{2}(p-1)}=\mathfrak{S}p+1$ ist, $(-3)^{\frac{1}{2}(p-1)}=\mathfrak{S}p-1$; und umgekehrt. Zu allen $p=4n-1$ also, zu welchen $+3$ Quadratrest ist, ist -3 Nichtquadratrest; und umgekehrt.

In (*L. c.*) ist $p=4n-1$, und $+3$ ist *Nichtquadratrest* zu $p=12n-5$; also ist -3 *Quadratrest* zu $p=12n-5$.

In (*L. d.*) ist $p=4n-1$, und $+3$ ist *Quadratrest* zu $p=12n-1$; also ist -3 *Nichtquadratrest* zu $p=12n-1$.

c. Zusammen also ist hier nach (*a.* und *b.*) -3 *Quadratrest* zu $p=12n+1$ und $p=12n-5$ und *Nichtquadratrest* zu $p=12n+5$ und $p=12n-1$; eben wie in (*M. c.*).

Anm. *O.* In (*B.* und *C.*) kommt eine Anwendung der Auflösung einer gewöhnlichen algebraischen Gleichung auf einen Zahlensatz vor; in dem zweiten Beweise eine Anwendung des Gegenseitigkeitsgesetzes.

§. 69.

Lehrsatz.

I. $+5$ *ist Quadratrest zu allen Stammzahlen* $p=10n+1$; *jedoch nicht zu diesen allein. Es ist also, wenn man*

$$1. \quad z^2=\mathfrak{S}p+5$$

setzt, wo z *die zwei Werthe* z *und* $p-z$ *oder* $+z$ *und* $-z$ *hat,* z *eine ganze Zahl* $>0<p-1$.

II. *Ferner ist dann auch für die beiden Werthe von* z *in* (1.)

$$2. \quad 2z-10 \text{ Quadratrest zu } p, \text{ für } p=10n+1,$$

nicht aber für andere Stammzahlen; so dafs also, wenn man für die beiden Werthe von z, *hier für* $p=10n+1$,

$$3. \quad y^2 = \mathfrak{S}p + 2z - 10$$

setzt, wo y *wiederum zwei Werthe* y *und* p — y *oder* + y *und* — y *hat, für jeden der beiden Werthe von* z, *also zusammen vier Werthe, auch* y *eine ganze Zahl* > 0 *und* < p — 1 *ist.*

III. *Die vier fünften Stammwurzeln aus* 1 *zu* p *sind*

$$4. \quad x_5 = \frac{\mathfrak{S}p - 1 + z + y}{4},$$

wenn man jeden der beiden Werthe von z *in* (1.) *je mit den beiden zu den andern Werthen von* z *gehörigen zwei Werthen von* y *in* (3.) *verbindet.*

IV. *Die vier zehnten Stammwurzeln aus* 1 *zu* p *sind*

$$5. \quad x_{10} = p - x_5.$$

Beispiel. Es sei $p = 61$, so ist nach Taf. I. für (1.):

$$6. \quad z = +26 \text{ und } +35 = p - 26, \text{ also } z = +26 \text{ und } -26.$$

Dieses giebt in (3.), Taf. I. zufolge,

$$7. \quad y^2 = \mathfrak{S}p + 2.26 - 10 = \mathfrak{S}p + 42, \text{ also } y = 15 \text{ und } 46 = p - 15 \text{ oder } y = +15 \text{ und } -15 \text{ für } z = +26, \text{ und}$$

$$8. \quad y^2 = \mathfrak{S}p - 2.26 - 10 = \mathfrak{S}p + 60, \text{ also } y = 11 \text{ und } 50 = p - 11 \text{ oder } y = +11 \text{ und } -11 \text{ für } z = -26.$$

Die beiden Werthe von y für den Werth +26 von z sind also +15 und —15, und die beiden Werthe von y für den Werth —26 von z sind +11 und —11.

Dieses giebt zufolge (III.) für die vier Werthe von x_5:

$$9. \begin{cases} 1. \quad x_5 = \frac{\mathfrak{S}p - 1 + 26 + 11}{4} = \frac{\mathfrak{S}p + 36}{4} = 9, \\ 2. \quad x_5 = \frac{\mathfrak{S}p - 1 + 26 - 11}{4} = \frac{\mathfrak{S}p + 14}{4} = \frac{2.61 + 14}{4} = \frac{136}{4} = 34; \\ 3. \quad x_5 = \frac{\mathfrak{S}p - 1 - 26 + 15}{4} = \frac{\mathfrak{S}p - 12}{4} = \frac{4.61 - 12}{4} = \frac{232}{4} = 58; \\ 4. \quad x_5 = \frac{\mathfrak{S}p - 1 - 26 - 15}{4} = \frac{\mathfrak{S}p - 42}{4} = \frac{2.61 - 42}{4} = \frac{80}{4} = 20; \end{cases}$$

und 9, 34, 58 und 20 sind, wie Taf. I. zeigt, die vier *fünften* Stammwurzeln aus 1 zu p.

Nach (5. 10.) und nach (9.) ist

$$10. \quad p - x = 61 - 9 = 52, \; 61 - 34 = 27, \; 61 - 58 = 3 \text{ und } 61 - 20 = 41,$$

und 52, 27, 3 und 41 sind, der Tafel zufolge, die *vier zehnten* Stammwurzeln aus 1 zu p.

Beweis. ***A.*** **Für die fünften Stammwurzeln aus 1 zu p ist**

$$11. \quad x^5 = \mathfrak{G}p+1.$$

Von den *fünf* ganzzahligen Werthen > 0 und $< p$, welche x für diese Gleichung nach (§. 54.) haben *kann*, und von welchen $x = 1$ einer ist, sind die vier andern, > 1, nothwendig die fünften *Stammwurzeln* aus 1 zu p, weil *vier* Zahlen 1, 2, 3 und 4 mit 5 keinen Theiler > 1 gemein haben und also, sobald $p-1$ mit 5, oder, weil $p-1$ immer *gerade* ist, mit 10 aufgeht, und folglich p von der Form $10n+1$ ist, nach (§. 63. I.) *vier* Stammwurzeln und folglich *vier* Werthe von $x > 1$ Statt finden *müssen*, die der Gleichung (11.) genugthun und die also die *vier andern* ganzzahligen Wurzeln der Gleichung (11.) sind, welche es aufser $x = 1$ geben kann und für $p = 10n+1$ geben *mufs*.

B. Diese vier Wurzeln der Gleichung (11.) > 1 sind die der Gleichung

$$12. \quad x^4+x^3+x^2+x+1 = np;$$

denn (11.) giebt

$$13. \quad x^5-1 = (x-1)(x^4+x^3+x^2+x+1) = \mathfrak{G}p,$$

und dieser Gleichung wird durch $x = 1$ und dann durch die vier andern Werthe, welche x in (12.) haben kann, entsprochen.

C. Dividirt man (12.) durch x^2, so ergiebt sich

$$14. \quad x^2+x+1+\frac{1}{x}+\frac{1}{x^2} = \frac{m}{x^2}.p.$$

Setzt man hierauf

$$15. \quad x+\frac{1}{x} = u,$$

welches $u^2 = x^2+2+\frac{1}{x^2}$, also $x^2+\frac{1}{x^2} = u^2-2$ giebt, so ist (14.) soviel als

$$u^2-2+u+1 = \frac{m}{x^2}.p \text{ oder}$$

$$16. \quad u^2+u-1 = \frac{m}{x^2}.p.$$

D. Löset man diese Gleichung zweiten Grades auf die gewöhnliche Weise auf, so findet sich $u = -\frac{1}{2}\pm\sqrt{\left(\frac{1}{4}+1-\frac{m}{x^2}.p\right)}$ oder

$$17. \quad 2u = -1\pm\sqrt{\left(5-\frac{4m}{x^2}.p\right)}.$$

Ferner giebt (15.) $x^2+1 = ux$ oder

$$18. \quad x^2-ux+1 = 0.$$

Löset man auch diese Gleichung zweiten Grades auf, so findet sich $x = +\frac{1}{2}u\pm\sqrt{(\frac{1}{4}u^2-1)}$ oder

$$19. \quad 4x = 2u\pm\sqrt{(4u^2-16)},$$

und hierin den Werth von $2u$ aus (17.) gesetzt,

$$4x = -1 \pm \sqrt{\left(5-\frac{4m}{x^2}.p\right)} \pm \sqrt{\left[1 \mp 2\sqrt{\left(5-\frac{4m}{x^2}.p\right)} + 5 - \frac{4m}{x^2}.p - 16\right]} \text{ oder}$$

$$20.\quad x = -\frac{1 \pm \sqrt{\left(5-\frac{4m}{x^2}.p\right)} \pm \sqrt{\left[-\frac{4m}{x^2}.p - 10 \mp 2\left(5-\frac{4m}{x^2}.p\right)\right]}}{4}$$

E. Nun muſs dieser Ausdruck von x nothwendig für $p = 10n+1$ *vier ganzzahlige* Werthe geben, weil dann vier ganzzahlige Stammwurzeln $x > 1$ aus 1 zu p Statt finden.

Dieses ist zunächst nicht anders möglich, als wenn das unbekannte $4m$ in (14.) mit x^2 *aufgeht;* denn wäre das nicht der Fall, so wäre in (20.) $\sqrt{\left(5-\frac{4m}{x^2}.p\right)}$ eine *Irrationalzahl,* oder doch ein *Bruch;* und Ähnliches wäre $\sqrt{\left[-\frac{4m}{x^2}\,p - 10 \mp 2\sqrt{\left(5-\frac{4m}{x^2}.p\right)}\right]}$. Es muſs also $-\frac{4m}{x^2}$ irgend eine *ganze* Zahl $\mathfrak{S}$ sein. Dadurch reducirt sich (20.) auf

$$21.\quad x = \frac{-1 \pm \sqrt{(\mathfrak{S}p+5)} \pm \sqrt{[\mathfrak{S}p - 10 \mp 2\sqrt{(\mathfrak{S}p+5)}]}}{4}.$$

F. Aber auch hier kann x nicht anders eine *ganze* Zahl sein, als wenn $\mathfrak{S}p+5$ irgend ein *Quadrat* z^2, also nach (1.)

$$22.\quad z^2 = \mathfrak{S}p+5$$

ist; denn wäre das nicht, so wäre wieder in (2.) $\sqrt{(\mathfrak{S}p+5)}$ eine *Irrationalzahl* und $\sqrt{[\mathfrak{S}p-10\mp 2\sqrt{(\mathfrak{S}p+5)}]}$ wäre es ebenfalls.

Dadurch reducirt sich dann (21.) auf

$$23.\quad x = \frac{-1 \pm z \pm \sqrt{(\mathfrak{S}p - 10 \mp 2z)}}{4}.$$

G. Hier ist wiederum aus denselben Gründen nöthig, daſs auch $\mathfrak{S}p-10\mp 2z$, oder, da für z in (22.) sowohl $+z$ als $-z$ gesetzt werden kann, $\mathfrak{S}p+2z-10$ irgend ein *Quadrat* y^2, folglich nach (3.)

$$24.\quad y^2 = \mathfrak{S}p+2z-10$$

sei; so daſs also nach (2.) nothwendig auch $2z-10$ *Quadratrest* zu p ist. Durch (24.) reducirt sich (23.), weil noch z sowohl $+z$ als $-z$ und y sowohl $+y$ als $-y$ ausdrückt, auf

$$25.\quad x = \frac{-1+z+y}{4}.$$

H. Die Gleichung (25.) giebt

$$26.\quad 4x = -1+z+y.$$

Aber wenn x der Gleichung (12.) genug thut, so thut es auch $\mathfrak{S}p+x$

Also kann man auch statt (26.)

$$27. \quad 4(\mathfrak{S}p+x) = -1+z+y$$

setzen, oder auch, wenn man $-\mathfrak{S}$ statt $4\mathfrak{S}$ schreibt,

$$28. \quad -\mathfrak{S}p+4x = -1+z+y,$$

und dies giebt schliefslich

$$29. \quad x = \frac{\mathfrak{S}p-1+z+y}{4};$$

welches der Ausdruck (4.) der vier fünften Stammwurzeln aus 1 zu p ist.

I. In (29.) oder (4.) mufs jeder der beiden Werthe, welche z in (2.) oder (1.) haben kann, *deshalb* je mit den beiden zu den *andern* Werthen von z gehörigen zwei Werthen von y in (3.) oder (24.) verbunden werden, damit für *jeden* Werth von x_5 in (4.) immer *alle* die verschiedenen Werthe von z und y in Rechnung kommen.

K. Was in (10.) von den vier *zehnten* Stammwurzeln aus 1 zu p behauptet wird, ist unmittelbar (§. 66. VI.) gemäfs.

L. Bekäme x in (21.) dadurch *allein,* dafs $+5$ Quadratrest zu p ist, *ganzzahlige* Werthe, so müfsten nothwendig *deshalb allein* fünfte Stammwurzeln aus 1 zu p Statt finden, und da dies *nur* dann der Fall ist, wenn $p-1$, aufser mit 2, mit 5 aufgeht, also $p=10n+1$ ist, so wäre der Umstand, dafs $+5$ Quadratrest zu p ist, auf die Stammzahlen $p=10n+1$ *beschränkt,* und keine andere Stammzahl $p=10n+3$, oder $p=10n-1$, oder $p=10n-3$ könnte $+5$ zum Quadratrest haben. Aber dies ist nicht der Fall. Dafs $+5$ Quadratrest zu p ist, reicht in (21.) nicht hin, sondern es mufs aufser $+5$ auch noch $2z-10$ Quadratrest zu p sein. Deshalb ist dann der Umstand, dafs $+5$ Quadratrest zu p ist, *nicht* auf die Stammzahlen $p=10n+1$ *beschränkt,* sondern auch *andere* Stammzahlen können $+5$ zum Quadratrest haben; wie in (I.) bemerkt.

M. Haben aber andere Stammzahlen als $p=10n+1$ zum Quadratrest $+5$, so kann zu ihnen $2z-10$ *nicht* Quadratrest sein; denn wäre das, so bekäme x in (21.) *nothwendig ganzzahlige* Werthe, und folglich fänden nothwendig auch für *solche* Stammzahlen fünfte Stammwurzeln aus 1 zu p Statt; was nicht der Fall ist, da für $p=10n-1$, $10n+3$ und $10n-3$, $p-1$ *nicht* mit 5 aufgeht. Dies wird in (II.) bemerkt.

Zu $p=29$ z. B. ist $+5$ Quadratrest und zwar zu $z=11$ und 18. Aber in $2z-10=2.11-10=12$, $=2.18-10=26$, $=2.-11-10 = -32 = \mathfrak{S}p+26 = 2.-18-10 = -46 = \mathfrak{S}p+12$ sind 12 und 26 *nicht* Quadratreste zu $p=29$.

Anm. *N.* Man könnte hier wieder, ähnlich wie im vorigen Paragraph, vermittels des Gegenseitigkeitsgesetzes für Quadratreste finden, *welche Form* p haben mufs, damit $+5$ oder auch -5 Quadratrest oder Nichtquadratrest zu p sei. Weiter unten kommt indessen ein *allgemeiner* Satz vor über die *Formen*, welche eine Stammzahl p haben mufs, damit eine *beliebige* gegebene positive oder negative Zahl x zu ihr Quadratrest oder Nichtquadratrest sei. Die Anwendung des Gegenseitigkeitsgesetzes auf den gegenwärtigen Fall $x = \pm 5$ kann also unterbleiben. Im vorigen Paragraph gab die Anwendung desselben auf $x = \pm 3$ schon das nöthige Beispiel. In dem gegenwärtigen und dem vorigen Paragraph kam es nur mehr auf die Ausdrücke der *fünften und dritten Stammwurzeln* aus 1 zu p an.

§. 70.

Aufgabe.

Die Reste, welche bleiben, wenn man die 2ten, 3ten, 4ten u. s. w. Potenzen einer beliebigen Zahl z durch eine andere gegebene Zahl $a > z$ dividirt, ohne Multiplication und Division, blofs durch Addition und Subtraction zu finden.

Beispiele für die Auflösung.

I. Es sei

1. $z = 6, \quad a = 33,$

2\. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32,
3\. 6 12 18 24 30 3 9 15 21 27 0 6 12 18 24 30 3 9 15 21 27 0 6 12 18 24 30 3 9 15 21 27,
4\. 6 3 18 9 21 27 30 15 24 12 6 3 18 9 21 27 30 15 24 12 6 3 18 9 21 27 30 15 24 12 6 3.

II. Es sei

5. $z = 15, \quad a = 41,$

6\. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40,
7\. 15 30 4 19 34 8 23 38 12 27 1 16 31 5 20 35 9 24 39 13 28 2 17 32 6 21 36 10 25 40 14 29 3 18 33 7 22 37 11 26,
8\. 15 20 13 31 14 5 34 18 24 32 29 25 6 8 38 37 22 2 30 40 26 21 28 10 27 36 7 23 17 9 12 16 35 33 3 4 19 39 11 1.

III. Es sei

9 $z = 23, \quad a = 41,$

10\. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40,
11\. 23 5 28 10 33 15 38 20 2 25 7 30 12 35 17 40 22 4 27 9 32 14 37 19 1 24 6 29 11 34 16 39 21 3 26 8 31 13 36 18,
12\. 23 37 31 16 40 18 4 10 25 1 23 37 31 16 40 18 4 10 25 1 23 37 31 16 40 18 4 10 25 1 23 37 31 16 40 18 4 10 25 1.

Auflösung, mit Beweis. *A.* Man schreibe die natürlichen Zahlen 1, 2, 3, 4 bis zu $a-1$ in eine horizontale Zeile (2. 6. 10.). Unter 1 setze man die Zahl z ($=6, 15, 23$), von welcher die Reste der verschiedenen Potenzen verlangt werden.

Man addire x zu sich selbst und setze die *Summe*, im Fall sie a nicht übersteigt, wie 12 und 30 in (3. und 7.), so wie sie ist, im Fall sie aber a übersteigt, wie in (11.), wo sie 46 ist, nachdem davon a *abgezogen* worden, den Rest (5 in (11.)) unter 2.

Zu dieser Summe addire man abermals x und setze die neue Summe, im Fall sie nicht a übersteigt, wie 18 und 28 in (3. und 11.), selbst, und im Fall sie a übersteigt, wie in (7.), wo sie 45 ist, nachdem davon a abgezogen worden, den Rest (4 in (7.)) unter 3.

Dasselbe Verfahren wiederhole man und setze das Resultat unter 4, und so fort, bis zu $a-1$.

Wie leicht zu sehen, enthält dann die zweite horizontale Zeile (3. 7. und 11.) die 1, 2, 3, 4, ...fachen der Zahl x; und zwar entweder diese Vielfachen selbst, oder die *Reste*, welche bleiben, wenn von den Vielfachen a so oft abgezogen wird, als es angeht.

B. Nun ist die 1te Potenz von x, x selbst. Man schreibe x ($=6, 15, 23$) in eine *dritte* horizontale Zeile (4. 8. 12.) unter die 1 der *ersten* Zeile (2. 6. 10.).

Die 2te Potenz von x ist das x*fache* von x. Man suche dieses x*fache*, welches sich nothwendig in der 2ten Zeile finden *mufs*, weil *alle* Vielfachen von x bis zu $a-1$fachen genommen worden sind und $x<a$ ist, in der *ersten* Zeile auf und schreibe es unter die Zahl 2 der ersten Zeile. In (I.) ist z. B. das $x=6$fache von 6 aufzusuchen, also 6 in der *ersten* Zeile. Unter dieser 6 steht 3, und dies ist der *Rest* zum 6fachen von 6, also von $6^2=x^2$. Die Zahl 3 setzt man daher unter die 2 der ersten Zeile in die dritte Zeile. In (II.) ist das 15fache von 15 aufzusuchen, also 15 in der *ersten* Zeile. Unter 15 steht 20, also ist 20 der *Rest* zum 15fachen von 15, folglich von $15^2=x^2$. Die Zahl 20 also mufs unter die 2 der ersten Zeile (6.) gesetzt werden; ähnlich in (III.).

Ferner ist die *dritte* Potenz von x das $x$fache von x^2; und da es blofs auf den *Rest* zu a ankommt, so ist der *Rest* für die dritte Potenz von x, den man verlangt, der Rest zum $x$fachen des *Restes* von x^2. Denn wenn $x^2=\mathfrak{G}a+r$ ist, so ist $x^3=\mathfrak{G}a+rx=\mathfrak{G}a+r_1$, wenn wieder $rx=\mathfrak{G}a+r_1$ ist. Man darf also nur den Rest zu x^2 (3 in (4.), 20 in (8.) und 37 in (12.)) in der ersten Zeile aufsuchen, so geben die in der zweiten Zeile darunter stehenden Zahlen (18 in (3.), 13 in (7.) und 31 in (11.)) das $x$fache des Restes zu x^2 und folglich den Rest zu x^3. Man schreibe daher diese Zahlen 18, 13 und 31 in die 3te Zeile (4. 8. und 12.) unter die 3 der ersten Zeile.

Nach *derselben* Regel sucht man wieder die für die Reste der 3ten Potenz von x so eben gefundenen Zahlen 18, 13 und 31 in der ersten Zeile (2. 6. und 10.) auf und schreibt die unter denselben in der *zweiten* Zeile (3. 7. und 11.) stehenden Zahlen 9, 31 und 16 in die *dritte* Zeile unter die 4. Sie sind die Reste zu der *vierten* Potenz von x.

Eben so weiter.

Die *dritte* Zeile (4. 8. 12.) enthält also nun die gesuchten Reste zu den *verschiedenen Potenzen* von x, deren *Exponenten* in der *ersten* Zeile darüber stehen. So ist z. B. zur 25ten Potenz von $x=6$ der Rest zu $a=33$ gemäfs (2. und 4.) $=21$. Der Rest zur 17ten Potenz von $x=15$ zu $a=41$ ist gemäfs (6. und 8.) $=22$; der Rest zur 28ten Potenz von $x=23$ zu $a=41$ ist gemäfs (10. und 12.) $=10$ u. s. w.

Es finden sich demnach auf solche Weise die Reste von allen Potenzen von x zu a *blofs* durch Addition und Subtraction, *ohne* alle Multiplication und Division.

Der *Proben* für die Rechnung giebt es mehrere.

C. Für die *zweite* Zeile ist es z. B. eine Probe, dafs zu den 2, 3fachen u. s. w. einer Zahl der *ersten* Zeile auch die 2, 3fachen u. s. w. der zugehörigen Zahlen in der *zweiten* Zeile gehören. Z. B. unter 7 in (2.) steht 9, also mufs unter $2.7=14$, $2.9=18$ unter $3.7=21$, $3.9=27$ stehen.

Ferner ist es eine Probe für die *zweite* Zeile, dafs, im Fall a *nicht* eine Stammzahl ist, sobald *eine* schon da gewesene Zahl der zweiten Zeile wiederkehrt, auch *alle folgenden* wiederkehren *müssen*; wie es sich in (3.) zeigt. Diesserhalb braucht man denn auch die zweite Zeile nur so weit zu berechnen, bis ihre *erste* Zahl wiederkehrt; alsdann kehren auch nothwendig die folgenden wieder. Ist a eine *Stammzahl*, oder auch nur eine zu x *theilerfremde* Zahl, so ist es eine Probe für die Zahlen der zweiten Zeile, dafs ihre erste Zahl, und überhaupt *keine* ihrer Zahlen, wiederkehren kann, weil alle Vielfachen einer Zahl zu einer andern ihr theilerfremden Zahl immer *verschiedene* Reste lassen. In solchem Fall müssen also die Zahlen der zweiten Zeile *alle* die Zahlen 1, 2, 3, 4, ... $a-1$ sein.

D. Für die *dritte* Zeile ist es eine Probe, dafs das *Product* zweier beliebigen ihrer Zahlen, durch a dividirt, zum Rest die Zahl geben mufs, über welcher in der *ersten* Zeile die *Summe* derjenigen Zahlen dieser Zeile steht, die sich über den beiden mit einander multiplicirten Zahlen der dritten Zeile befinden. Denn wenn z. B. $x^m=\mathfrak{G}a+r_m$ und $x^n=\mathfrak{G}a+r_n$ ist, so stehen

die Exponenten m und n in der *ersten* Zeile und die Reste r_m und r_n in der *dritten*. Die beiden Gleichungen mit einander multiplicirt, giebt aber $x^{m+n} = \mathfrak{S}a + r_m r_n$, also mufs unter der Zahl $m+n$ der ersten Zeile, oder, wenn $m+n > a-1$ und a eine *Stammzahl* ist, unter $m+n-(a-1)$, in der dritten Zeile das Product $r_m r_n$ stehen, und wenn $r_m r_n > a$ und a eine *Stammzahl* ist, $r_m r_n - \mathfrak{S}a$; denn die Zahlen der dritten Zeile sind die *Reste* zu a, und von den höheren Potenzen von x als der $a-1$ten für eine Stammzahl a ist schon die $a$te der 1ten gleich, weil dann nach dem Fermatschen Lehrsatz für *jedes* x, $x^{a-1} = \mathfrak{S}p + 1$ ist, so dafs also die $(m+n-(a-1))$ten Potenzen dieselben Reste haben wie die $(m-n)$ten. Z. B. unter 8 in (10.) steht in der dritten Zeile 10 und unter 17 steht 4, also mufs unter $8+17=25$ in der dritten Zeile $10.4=40$ stehen; und so ist es auch. Unter 14 in (6.) steht in der dritten Zeile 8 und unter 37 steht 19, also mufs unter $14+37 = 51 = \mathfrak{S}41+11$, mithin unter der 11 der ersten Zeile $8.19 = 152 = 3.41+29$, also 29 stehen; was auch der Fall ist.

Ferner findet für die *dritte* Zeile auch eine ähnliche Probe Statt, wie für die zweite. Nemlich wenn die *erste* Zahl der dritten Zeile *wieder*kehrt, so müssen auch alle folgenden wiederkehren; denn wenn z. B. in $x^m = \mathfrak{S}p + r$, $r = x$ ist, so ist offenbar $x^{m+1} = \mathfrak{S}p + x^2$, $x^{m+2} = \mathfrak{S}p + x^3$ u. s. w., und x^{m+1}, x^{m+2} u. s. w. lassen also *dieselben* Reste zu a wie x^2, x^3, sobald x^m zu a den Rest von x^1 giebt. So zeigt es sich in (4. und 12.).

Ist a eine *Stammzahl* und x eine der *Hauptstammwurzeln* zu a, so kann in der dritten Zeile die erste Zahl derselben gar nicht wiederkehren; denn alle Potenzen von x geben dann verschiedene Reste. Die Zahlen der dritten Zeile müssen also in diesem Fall *alle* die Zahlen 1, 2, 3, ... $a-1$ sein, wie es sich auch z. B. in (8.) zeigt. Auch mufs, wenn a eine Stammzahl ist, unter $a-1$ der ersten Zeile, dem Fermatschen Lehrsatze gemäfs, in der dritten Zeile *immer* 1 stehen.

§. 71.

Aufgabe.

Die Reste zu berechnen, welche bleiben, wenn man eine und dieselbe, z. B. die $e$te Potenz der Zahlen 1, 2, 3, 4, ... mit der Zahl a dividirt, und welche $< a$ sind.

Auflösung mit Beispielen und Beweis. *A.* Es sei x eine beliebige Zahl, also eine derer 1, 2, 3, 4, ..., von welcher die Reste der $e$ten Potenz zu a gesucht werden; so erhält man zunächst den Rest r_1 der

2ten Potenz von z zu a, wenn man z mit sich selbst multiplicirt und das Product mit a dividirt. Darauf erhält man den Rest r_4 der 4ten Potenz von z zu a, wenn man r_2 mit sich selbst multiplicirt und das Product durch a dividirt; denn wenn $z^2 = \mathfrak{G}a + r_2$ ist, so ist $z^4 = (\mathfrak{G}a + r_2)^2 = \mathfrak{G}a + r_2^2 = \mathfrak{G}a + r_4$. Aus gleichem Grunde erhält man den Rest r_8 zur $2^3 = 8$ten Potenz von z zu a, wenn man r_4 mit sich selbst multiplicirt und das Product mit a dividirt. Und so weiter die Reste r_{16}, r_{32}, r_{64}, ... der 2^4ten, 2^5ten etc. Potenzen von z zu a.

B. Nun kann nach (§. 31.) *jede* Zahl blofs durch Summirung verschiedener Potenzen *der Zahl* 2 zusammengesetzt werden. Welcher also auch der Exponent e sein mag, für den man r in

$$1. \quad z^e = \mathfrak{G}a + r$$

verlangt: immer ist derselbe die *Summe* dieser oder jener Potenzen von 2. Man darf also nur die vorhin gefundenen Reste derjenigen Potenzen von z, deren Exponenten jene Potenzen von 2 sind, welche summirt e geben, mit einander multipliciren, so findet sich das gesuchte r in (1.). Wenn z. B. $e = x_1 + x_2 + x_3 \ldots.$ und $z^{x_1} = \mathfrak{G}a + r_1$, $z^{x_2} = \mathfrak{G}a + r_2$, $z^{x_3} = \mathfrak{G}a + r_3$ etc. ist, so ist

$$2. \quad z^e = z^{x_1+x_2+x_3\ldots} = z^{x_1}.z^{x_2}.z^{x_3}\ldots = (\mathfrak{G}a + r_1)(\mathfrak{G}a + r_2)(\mathfrak{G}a + r_3)\ldots$$
$$= \mathfrak{G}a + r_1 r_2 r_3 \ldots,$$

und folglich vermöge (1.) $r = r_1 r_2 r_3 \ldots$ oder, wenn $r_1 r_2 r_3 \ldots > a$ ist,

$$3. \quad r_1 r_2 r_3 \ldots = \mathfrak{G}a + r.$$

Gesetzt e sei 53, so ist $e = 32 + 16 + 4 + 1 = 2^0 + 2^2 + 2^4 + 2^5$. Verlangte man also den Rest der 53ten Potenz der Zahl $z = 7$ zu $a = 55$, so wäre zunächst $z^2 = 7^2 = 49$, $z^4 = 49^2 = (55-6)^2 = \mathfrak{G}.a + 36$, $z^8 = 36^2 = \mathfrak{G}a + 31$, $z^{16} = 31^2 = \mathfrak{G}a + 26$, $z^{32} = 26^2 = \mathfrak{G}a + 16$, und da nun $e = 1 + 4 + 16 + 32$ ist, so ergiebt sich aus (3.) $\mathfrak{G}a + r = 7.36.26.16$, also $r = 2$.

C. Nach diesem Verfahren nun berechne man von den $e$ten Potenzen der *Stammzahlen* 2, 3, 5, 7, 11, ... die Reste zu a. Aus den Resten der $e$ten Potenzen *dieser* $z = 2, 3, 5, 7, 11, \ldots$ lassen sich die Reste *aller übrigen* z durch Multiplication mit einander finden, weil *jede* Zahl ein *Product von Stammzahlen* ist. Wären nemlich r_1, r_2, r_3, ... die für die Stammzahlen p_1, p_2, p_3, ... gefundenen Reste zu a, so dafs

$$4. \quad p_1^e = \mathfrak{G}a + r_1, \quad p_2^e = \mathfrak{G}a + r_2, \quad p_3^e = \mathfrak{G}a + r_3, \quad \ldots.$$

und es würde irgend eine Zahl z durch

$$5. \quad z = p_1^{\varepsilon_1}.p_2^{\varepsilon_2}.p_3^{\varepsilon_3}\ldots,$$

bezeichnet, so wäre

$$6. \quad z^e = p_1^{e\varepsilon_1}.p_2^{e\varepsilon_2}.p_3^{e\varepsilon_3}\ldots = (\mathfrak{G}a+r_1)^{\varepsilon_1}(\mathfrak{G}a+r_2)^{\varepsilon_2}(\mathfrak{G}a+r_3)^{\varepsilon_3}\ldots$$
$$= \mathfrak{G}a+r_1^{\varepsilon_1}r_2^{\varepsilon_2}r_3^{\varepsilon_3}\ldots$$

und folglich für (1.)

$$7. \quad r+\mathfrak{G}a = r_1^{\varepsilon_1}r_2^{\varepsilon_2}r_3^{\varepsilon_3}\ldots$$

Der Rest der $e=53$ten Potenz von $p_1=7$ zu $55=a$ war z. B. in (*B.*) $r_1=2$. Für den Rest der $53=e$ten Potenz von $p_2=3$ zu $55=a$ findet sich $r_2=48$. Aus diesen beiden Resten $r_1=2$ und $r_2=48$ finden sich also durch (7.) schon die Reste der $e=53$ten Potenzen zu a von allen den z, welche (5.) ausdrückt. Z. B. für $\varepsilon_1=3$, $\varepsilon_2=2$ giebt (5.) $z=7^3.3^2$ $=3087$ und (7.) giebt $r+\mathfrak{G}a=2^3.48^2=8.(-7)^2=7$; also ist 7 der Rest der $e=53$ten Potenz von $z=3087$ zu $a=55$.

D. Verlangt man nun von den Zahlen $z=1,2,3,4,\ldots$ *bis zu* a die Reste der $e$ten Potenzen zu a, so kann man statt (5.)

$$8. \quad z = p_1^{\varepsilon_1}r_2^{\varepsilon_2}r_3^{\varepsilon_3}\ldots+\mathfrak{G}a$$

setzen, wo $\mathfrak{G}$ so anzunehmen ist, dafs $z<a$ bleibt. Alsdann lassen sich schon aus den nach (*B.*) berechneten Resten r_1, r_2, r_3, ... für wenige Stammzahlen p_1, p_2, p_3, ..., ja selbst schon aus den Resten für eine einzelne Stammzahl p, die Reste für viele z finden.

Hätte man z. B. nach (*B.*) blofs für die eine, kleinste Stammzahl $p_1=2$ den Rest der $e=53$ten Potenz zu $a=55$ berechnet, welcher $r_1=52=\mathfrak{G}p-3$ ist, so giebt derselbe nach (7.) schon allein die Reste zu $z^2=(-3)^2=9$, $z^3=(-3)^3=-27=+28$, $z^4=-3.28=-84=+26$, $z^5=-3.26$ $=-78=+32$ u. s. w.

E. Ist a eine *Stammzahl* und man verlangt die Reste der $e$ten Potenzen von $z=1,2,3,4,\ldots a-1$ zu a, so braucht man nach dem obigen Verfahren nur die Reste für die *Hälfte* der z, nemlich nur für $z=$ $1,2,3,4,\ldots \frac{1}{2}(a-1)$ und also jedenfalls auch nur für die *Stammzahlen* $<\frac{1}{2}a$ zu berechnen; denn die Reste für die folgenden z, bis zu a, sind nach (§. 55. III.) die berechneten Reste selbst, in umgekehrter Aufeinanderfolge, wenn e *gerade*, und die Ergänzungen derselben zu a, wenn e *ungerade* ist.

§. 72.

Aufgabe.

Die sämmtlichen *Stammwurzeln*, also auch die *Hauptstammwurzeln*, zu einer gegebenen *Stammzahl* p zu berechnen.

Auflösung mit Beweis und Beispielen. *A.* Da nach (§. 63. IV.) die Reste der verschiedenen Potenzen jeder *Hauptstammwurzel* unmittelbar nicht allein die übrigen Hauptstammwurzeln, sondern auch alle andern Stammwurzeln für alle die Exponenten δ geben, die in $p-1$ aufgehen, so kommt es offenbar nur darauf an, *irgend eine der Hauptstammwurzeln* zu finden. Kennt man eine solche, so darf man nur die Reste ihrer verschiedenen Potenzen bis zur $p-1$ten zu p berechnen; was nach (§. 70.) durch bloße Addition und Subtraction, also *sehr leicht* geschieht, und die Aufgabe wird weiter nach den Regeln von (§. 63. IV.) ohne viele Mühe vollständig gelöset.

B. Aber die Schwierigkeit ist, *eine* der Hauptstammwurzeln zu finden. Wie dies *ohne Versuche* mit Leichtigkeit geschehen könne, ist eine noch nicht gelösete Aufgabe.

C. Ein Mittel, nicht sowohl eine, sondern sogleich alle *Hauptstammwurzeln ohne* Versuche zu finden, ist freilich folgendes; aber es erfordert, wenn p groß ist, *viele* Rechnung.

Nach (§. 64. III.) erhält man nemlich die Hauptstammwurzeln, wenn man von den Zahlen 1, 2, 3, 4, ... $p-1$ die Reste derjenigen ihrer Potenzen *ausschließt*, deren Exponenten $\lambda_1, \lambda_2, \lambda_3, \ldots$ die in $p-1$ aufgehenden *Stammzahlen* sind. Man müßte also die Reste r in

$$1. \quad z^{\lambda} = \mathfrak{G}p + r$$

für alle die $z = 1, 2, 3, 4, \ldots p-1$, und für alle λ, welche in $p-1$ aufgehende *Stammzahlen* sind, berechnen; was nach (§. 71.) geschehen könnte. Aber diese Rechnung ist sehr weitläuftig, wenn p beträchtlich groß ist. Auch hätte man dann erst die *Hauptstammwurzeln*, und müßte, wenn man auch noch die übrigen Stammwurzeln verlangt, dennoch nach (*A.*) noch erst weiter die Reste aller Potenzen einer von ihnen bis zur $p-1$ten berechnen; woraus dann nach (§. 63. IV.) die übrigen Stammwurzeln sich ergeben würden.

D. Daher wird man, besonders für beträchtlich große p, immer noch leichter zum Ziele gelangen, wenn man durch *Versuche* erst *bloß eine* Hauptstammwurzel zu ermitteln sucht. Ist diese gefunden, so ergiebt sich nach (*A.*) unmittelbar und leicht das Übrige.

Zu diesen Versuchen kann und wird man also die *kleinsten* Zahlen 2, 3, 5, 6, 7, 8, 10, ... nehmen, nicht 4, 9, 16 etc., denn diese sind *Quadratreste*, und kein Quadratrest ist eine Hauptstammwurzel (§. 66. III. *a.*).

Dabei lassen sich dann aber noch einige der obigen Lehrsätze von den Stammwurzeln zur Verminderung der Rechnung benutzen.

E. Gesetzt das gegebene p sei

$$2.\quad p = 541,\ \text{also}\ p-1 = 540 = 2^2.3^3.5.$$

Man setze

$$3.\quad z^x = \mathfrak{G}p + r$$

und lasse x die verschiedenen *Theiler* von $p-1$ bezeichnen, so dafs

$$4.\quad x = 2,3,4,5,6,9,10,12,15,18,20,27,30,36,45,54,60,90,108,135,180\ \text{und}\ 270$$

ist, so mufs nach (§. 66. VII.), wenn in (3.) z eine *Hauptstammwurzel*, das heifst eine $\delta = p-1$te Stammwurzel sein soll, erstlich für $x = \frac{1}{2}(p-1)$, $r = -1$ sein, und zweitens mufs für alle x, die *nur* in $p-1$, *nicht* in $\frac{1}{2}(p-1)$ aufgehen, r weder $+1$ noch -1 sein. Es mufs also hier für $p-1 = 540$ zunächst r in (3.) für $x = 270$ gleich -1, und dann mufs für $x = 4$, 12, 20, 36, 60, 108 und 180, welches die x sind, die *nur* in $p-1$, *nicht* in $\frac{1}{2}(p-1)$ aufgehen, r in (3.) weder $+1$ noch -1 sein.

Wollte man also nun versuchen, ob $z = 2$ eine Hauptstammwurzel zu $p = 541$ sei, so kommt es auf die 4, 12, 20, 36, 60, 108, 180 und 270ten *Potenzen von* 2 und auf ihre Reste zu p an. Es ergiebt sich $2^4 = 16$, $2^8 = 256$, $2^{12} = 2^4.2^8 = 16.256 = \mathfrak{G}p + 309$, $2^{20} = 2^8.2^{12} = 256.309 = \mathfrak{G}p + 118$, $2^{36} = 2^{12.3} = 309^3 = \mathfrak{G}p + 194$, $2^{60} = 2^{20.3} = 118^3 = \mathfrak{G}p + 15$, $2^{108} = 2^{36.3} = 194^3 = \mathfrak{G}p + 48$, $2^{180} = 2^{60.3} = 15^3 = \mathfrak{G}p + 129$. Die Rechnung wird erleichtert, wenn man *Potenzen-Tafeln* hat; z. B. diejenigen von *Vega.* Keiner der Reste zu p von der 4, 12, 20, 36, 60 und 180ten Potenz von 2 ist also weder $+1$ noch -1, und wenn man nun noch $2^{270} = 2^{180}.2^{60}.2^{20}.2^8.2^2 = 129.15.118.256.4$ berechnet, so findet sich $2^{270} = \mathfrak{G}p - 1$. Also ist $z = 2$ in der That eine der *Hauptstammwurzeln* zu $p = 541$.

Man berechne nun noch die Reste zu den verschiedenen Potenzen von 2 bis zu $p-1 = 540$ nach (§. 70.), was durch blofse Addition und Subtraction leicht ist, so lassen sich weiter aus denselben nach der Regel (§. 63. IV.) die sämmtlichen Hauptstammwurzeln, so wie die übrigen Stammwurzeln, unmittelbar entnehmen.

F. Fände sich, anders wie in dem Fall (*E.*) für $p = 541$, dafs $z = 2$ *nicht* eine Hauptstammwurzel ist, so versuche man die nächste Zahl $z = 3$

Findet sich, dafs auch 3 keine Hauptstammwurzel ist, so versuche man $x = 5$ u. s. w. Aber schon, wenn die zwei Zahlen 2 und 3 versucht sind, lassen sich wieder andere Lehrsätze zur Verminderung der weitern Rechnung benutzen.

Es sei z. B.

$$5.\quad p = 41, \quad \text{also} \quad p - 1 = 40.$$

Hier sind die *Theiler* x von $p-1$ folgende:

$$6.\quad x = 2,\ 4,\ 5,\ 8,\ 10 \text{ und } 20,$$

und von diesen geht nur allein 8 in $p-1$ und nicht in $\frac{1}{2}(p-1)$ auf, also kommt es für $x = 2$, nächst $2^{\frac{1}{2}(p-1)} = 2^{20}$, nur auf 2^8 an. Es ist $2^8 = 16^2 = 256 = \mathfrak{G}p + 10$. Dies ist zwar weder $+1$ noch -1, aber $2^{\frac{1}{2}(p-1)} = 2^{20}$ ist $2^{2 \cdot 8} . 2^4 = 10^2 . 16 = 1600 = \mathfrak{G}p + 1$, nicht $\mathfrak{G}p - 1$, wie es sein soll; also ist 2 *nicht* eine Hauptstammwurzel zu $p = 41$. Man versuche also $x = 3$. Dieses giebt $3^2 = 9$, $3^4 = 81 = \mathfrak{G}p - 1$, $3^8 = \mathfrak{G}p + 1$, $3^{16} = \mathfrak{G}p + 1$, $3^{20} = \mathfrak{G}p - 1$; also ist auch 3 keine Hauptstammwurzel zu $p = 41$. Aber es ist nun nicht weiter nöthig, noch eine andere Zahl für x zu versuchen, denn aus $2^8 = \mathfrak{G}p + 10$, $2^{20} = \mathfrak{G}p + 1$, $3^8 = \mathfrak{G}p + 1$ und $3^{20} = \mathfrak{G}p - 1$ folgt $(2.3)^8 = 6^8 = \mathfrak{G}p + 10$ und $(2.3)^{20} = 6^{20} = \mathfrak{G}p - 1$: folglich ist 6 *nothwendig* eine der Hauptstammwurzeln zu $p = 41$.

Man hat also nun nach (§. 70.) die Reste der Potenzen von 6 zu berechnen. Dies giebt:

7.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40,
8.	6	12	18	24	30	36	1	7	13	19	25	31	37	2	8	14	20	26	32	38	3	9	15	21	27	33	39	4	10	16	22	28	34	40	5	11	17	23	29	35,
9.	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33	34	40	35	5	30	16	14	2	12	31	22	9	13	37	17	20	38	23	15	8	7	1.

Die Zahlen in der Reihe (9.) sind die verlangten Reste.

Nun sind die zu $p - 1 = 40$ *theilerfremde* Zahlen > 1 folgende: 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37 und 39. Zu diesen Zahlen in der Reihe (7.) gehören in der Reihe (9.) die Zahlen

10. 6, 11, 29, 19, 28, 24, 26, 34, 35, 30, 12, 22, 13, 17, 15 und 7.

Diese sind also nach (§. 63. IV.) die Hauptstammwurzeln aus 1 zu $p = 41$.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{20} = 2$ haben, sind 2, 6, 14, 18, 22, 26, 34 und 38. Zu diesen Zahlen in der Reihe (7.) gehören in der Reihe (9.) die Zahlen

11. 36, 39, 21, 33, 5, 2, 20 und 8.

Diese sind also nach (§. 63. IV.) die 20ten Stammwurzeln aus 1 zu p.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{10} = 4$ haben, sind 4, 12, 28 und 36. Diese aus (7.) geben in (9.)

die Zahlen

12. 25, 4, 31 und 23;

welches die 10ten Stammwurzeln aus 1 zu p sind.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{5}=8$ haben, sind 8, 16, 24 und 32. Zu ihnen in (7.) gehören in (9.) die Zahlen

13. 10, 18, 16 und 37;

und dieses sind die 5ten Stammwurzeln aus 1 zu p.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40, zum gröfsten Gemeintheiler $\frac{p-1}{8}=5$ haben, sind 5, 15, 25 und 35. Zu ihnen in (7.) gehören in (9.) die Zahlen

14. 27, 3, 14 und 38;

und dies sind die 8ten Stammwurzeln aus 1 zu p.

Die Zahlen, welche mit 1, 2, 3, 4, ... 40 zum gröfsten Gemeintheiler $\frac{p-1}{4}=10$ haben, sind 10 und 30. Zu ihnen in (7.) gehören in (9.) die Zahlen

15. 32 und 9;

und dieses sind die 4ten Stammwurzeln aus 1 zu p.

Endlich ist $p-1=40$ die 2te und 1 die erste Stammwurzel aus 1 zu p. Also sind auf diese Weise *alle* Stammwurzeln aus 1 zu p vermittels der einen Hauptstammwurzel 6 gefunden worden.

G. Meistens wird schon der Versuch von weniger kleinen Zahlen für x hinreichen, um eine der Hauptstammwurzeln zu entdecken, und die übrige Rechnung ist dann nach der obigen Art leicht; so dafs also diese Art der Auflösung der Aufgabe meistens ohne zu grofse Mühe anwendbar ist.

Nach ihr ist die Tafel im 9ten Bande dieses Journals S. 36 — 53 für die Stammzahlen bis 101 berechnet worden. Zugleich giebt diese Tafel die Reste der Potenzen von 1, 2, 3, 4, ... $p-1$, deren Exponenten die in $p-1$ aufgehenden *Stammzahlen* sind, an; auch noch, bis zu $p=29$, die Reste der Potenzen von 1, 2, 3, 4, ... $p-1$ für *alle* Exponenten von 2 bis $p-1$, nebst den Werthen von x, zu welchen die Reste gehören. Da die Tafel überall die positiven *Quadratreste* angiebt, so kann man daraus nach (§. 45.) auch unmittelbar die *negativen* Quadratreste, so wie die positiven und negativen *Nichtquadratreste* entnehmen. Die weiter folgende Tafel giebt an, zu welchen Stammzahlen von 3 bis 101 die Zahlen 2, 3, 4, 5, ... 100 Hauptstammwurzeln sind.

§. 73.

Andere Beweise des Wilsonschen Lehrsatzes (§. 48.), nemlich:
Dafs für jede Stammzahl $p>1$ das Product

$$1.\quad 1.2.3.4\ldots(p-1) = \mathfrak{G}p-1$$

ist.

Zweiter Beweis, durch Quadratreste und Nichtquadratreste.

A. Man setze

$$2.\quad (p-1)^2=\mathfrak{G}p+r_1,\quad (p-2)^2=\mathfrak{G}p+r_2,\quad (p-3)^2=\mathfrak{G}p+r_3,\ \ldots\ldots \tfrac{1}{2}(p+1)^2=\mathfrak{G}p+r_{\frac{1}{2}(p+1)}.$$

Die r in (2.) sind *alle* verschiedenen *Quadratreste* zu p (§. 45. 5. und 6.). Die Gleichungen

$$3.\quad 1^2=\mathfrak{G}p+r_1,\quad 2^2=\mathfrak{G}p+r_2,\quad 3^2=\mathfrak{G}p+r_3,\ \ldots\ldots \tfrac{1}{2}(p-1)^2=\mathfrak{G}p+r_{\frac{1}{2}(p-1)}$$

geben *dieselben* r, wenn auch in verschiedener Aufeinanderfolge (§. 45. 5.)

B. Nun ist das *Product* eines *Quadratrestes* und eines *Nichtquadratrestes* ein *Nichtquadratrest* (§. 52. IV.). Multiplicirt man also z. B. $1^2=\mathfrak{G}p+r_1$ mit irgend einem *Nichtquadratrest* ϱ_m, so erhält man $\varrho_m.1^2=\mathfrak{G}p+\varrho_1$, wo ϱ_1 irgend ein *Nichtquadratrest* ist. Multiplicirt man $2^2=\mathfrak{G}p+r_2$ mit *demselben* Nichtquadratrest ϱ_m, so ist in $\varrho_m.2^2=\mathfrak{G}p+\varrho_2$, ϱ_2 irgend ein *anderer* Nichtquadratrest als ϱ_1, weil r_2 ein *anderes* r als r_1 ist. U. s. w. Also wenn man *alle* die Gleichungen (3.) mit *einem und demselben* Nichtquadratrest ϱ_m multiplicirt, so erhält man durch

$$4.\quad \varrho_m.1^2=\mathfrak{G}p+\varrho_1,\quad \varrho_m.2^2=\mathfrak{G}p+\varrho_2,\quad \varrho_m.3^2=\mathfrak{G}p+\varrho_3,\ \ldots\ldots \varrho_m(p-1)^2=\mathfrak{G}p+\varrho_{\frac{1}{2}(p-1)}$$

$\frac{1}{2}(p-1)$ *verschiedene* und folglich *alle Nichtquadratreste* ϱ, indem es deren nur $\frac{1}{2}(p-1)$ giebt, nemlich so viele als *Quadratreste* r.

C. Multiplicirt man nun die sämmtlichen Gleichungen (4.) in einander, so ergiebt sich

$$5.\quad \varrho_m^{\frac{1}{2}(p-1)}(1.2.3.4\ldots.\tfrac{1}{2}(p-1))^2 = \mathfrak{G}p+\varrho_1\varrho_2\varrho_3\ldots.\varrho_{\frac{1}{2}(p-1)}.$$

Nun ist für *jeden Nichtquadratrest* ϱ, nach (§. 49. 2.),

$$6.\quad \varrho_m^{\frac{1}{2}(p-1)} = \mathfrak{G}p-1,$$

also giebt (5.)

$$(\mathfrak{G}p-1)(1.2.3.4\ldots.\tfrac{1}{2}(p-1))^2 = \mathfrak{G}p+\varrho_1\varrho_2\varrho_3\ldots.\varrho_{\frac{1}{2}(p-1)} \text{ oder}$$

$$7.\quad -(1.2.3.4\ldots.\tfrac{1}{2}(p-1))^2 = \mathfrak{G}p+\varrho_1\varrho_2\varrho_3\ldots.\varrho_{\frac{1}{2}(p-1)}.$$

D. Multiplicirt man die Gleichungen (2.) in einander, so erhält man

$$8.\quad ((p-1)(p-2)(p-3)\ldots.\tfrac{1}{2}(p+1))^2 = \mathfrak{G}p+r_1r_2r_3\ldots.r_{\frac{1}{2}(p-1)};$$

und dieses mit (7.) multiplicirt, giebt, weil nun in dem Product *alle* die Zahlen 1, 2, 3, 4, ... $p-1$ vorkommen,

9. $-(1.2.3.4\ldots(p-1))^2 = \mathfrak{G}p + r_1 r_2 r_3 \ldots r_{\frac{1}{2}(p-1)} \varrho_1 \varrho_2 \varrho_3 \ldots \varrho_{\frac{1}{2}(p-1)}$.

E. Aber in (9.) sind rechterhand $r_1, r_2, r_3, \ldots r_{\frac{1}{2}(p-1)}, \varrho_1, \varrho_2, \varrho_3, \ldots \varrho_{\frac{1}{2}(p-1)}$ ebenfalls alle die Zahlen 1, 2, 3, 4, ... $p-1$, denn ihre Gesammtzahl ist $p-1$, und sie sind *alle verschieden*. Also giebt (9.)

$$-(1.2.3.4\ldots(p-1))^2 = \mathfrak{G}p + 1.2.3.4\ldots p-1 \text{ oder}$$

10. $-(1.2.3.4\ldots(p-1))[1.2.3.4\ldots(p-1)+1] = \mathfrak{G}p$.

F. Es mufs also p entweder in den Factor $1.2.3.4\ldots p-1$, oder in den Factor $1.2.3.4\ldots(p-1)+1$ *aufgehn*. In den ersten Factor geht es *nicht* auf, weil die einzelnen Factoren 1, 2, 3, 4, ... $p-1$ alle *kleiner als p* sind: also mufs p in den zweiten Factor aufgehen, und daher mufs

11. $1.2.3.4\ldots(p-1)+1 = \mathfrak{G}p$

sein; woraus die Gleichung (1.) des Lehrsatzes folgt.

Dritter Beweis, durch Hauptstammwurzeln. *G.* Es sei z eine *Hauptstammwurzel* aus 1 zu p und

12. $z^x = \mathfrak{G}p + r$,

so durchläuft nach (§. 50. II.), wenn man

13. $x = 1, 2, 3, 4, \ldots p-1$

setzt, der Rest r ebenfalls *alle* die Zahlen 1, 2, 3, 4, ... $p-1$.

H. Nun ist nach (§. 67. II.) das Product aller Reste einer δten *Stammwurzel* $= \mathfrak{G}p+1$, wenn δ *ungerade*, und $= \mathfrak{G}p-1$, wenn δ *gerade* ist. Für die *Hauptstammwurzeln* ist $\delta = p-1$ *immer* gerade, also ist für die Hauptstammwurzel

14. $1.2.3.4\ldots p-1 = \mathfrak{G}p-1$;

und dies ist der Wilsonsche Satz.

Vierter Beweis, durch zusammengehörige Zahlen und Quadratreste. *L.* Aus den Zahlen

15. $z = 1, 2, 3, 4, \ldots p-1$

geben *je zwei* Zahlen z_1 und z_2 aus denen (15.) gemäfs (§. 47. III.)

16. $z_1 z_2 = \mathfrak{G}p + \varrho$,

wo ϱ ein beliebiger *Nichtquadratrest* zu p ist. Es sind nach (§. 47. III.) $\frac{1}{2}(p-1)$ solche Producte vorhanden, und in ihnen durchlaufen die z_1 und z_2 *alle* die Zahlen (15.), ohne dafs irgend eine mehr als einmal vorkäme.

M. Daraus folgt, dafs das Product aller der $\frac{1}{2}(p-1)$ Producte (16.) das Product *aller* der Zahlen (15.) ist; und da nun *jedes* der $\frac{1}{2}(p-1)$ Pro-

ducte (16.) $= \mathfrak{G}p + \rho$ giebt, so ist

$$17. \quad 1.2.3.4\ldots.(p-1) = \mathfrak{G}p + \rho^{\frac{1}{2}(p-1)}.$$

N. Aber für jeden *Nichtquadratrest* ρ ist zufolge (§. 49. I.), und zwar zufolge des *ersten* Beweises daselbst, der *nicht* auf dem Wilsonschen Satze beruht,

$$18. \quad \rho^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1,$$

also ist nach (17.)

$$19. \quad 1.2.3.4\ldots.(p-1) = \mathfrak{G}p - 1;$$

dem Lehrsatze gemäfs.

Weiter unten werden sich noch andere, auf andern Vordersätzen beruhende Beweise des Satzes finden.

(Die Fortsetzung folgt.)

14.

Eine allgemeine Formel für die gesammte jüdische Kalenderberechnung.

(Von Herrn *Ch. Z. Slonimsky* aus Bialystock in Rufsland.)

Die sonderbare aber kunstreiche Einrichtung des jüdischen Kalenders, welche in ihrer Künstlichkeit wohl die einzige in der ganzen Chronologie ist, bietet dem Chronologen wegen der weitläuftigen Berechnungen und besondern Ausnahmen viele Schwierigkeiten dar. Alle unsere Chronologen, welche diesen Kalender beschrieben und erläutert haben, mufsten beim practischen Gebrauch desselben nach der traditionellen und gewöhnlichen Weise die Berechnungen anstellen; welches aber nicht blofs schwierig ist, wegen des Gebrauchs ungewöhnlich benannter Zahlen und der Hülfstabellen, sondern auch ungenügend; indem man dessenungeachtet nicht im Stande ist, das verlangte Jahr direct zu bestimmen. Da es nemlich im jüdischen Kalender sechs verschiedene Jahreslängen giebt, so müssen erst die zwei aufeinanderfolgenden Neujahrstage gefunden werden, um die Länge des zu Grunde gelegten Jahres bestimmen zu können; welches die eigentliche Aufgabe des Kalenders ist. Auf noch gröfsere Schwierigkeiten stöfst man bei der Berechnung des jüdischen Kalenders in der christlichen Zeitrechnung.

Die bekannte Formel, welche der Herr Prof. *Gaufs* zur Berechnung des jüdischen Osterfestes aufstellte, hat, ungeachtet der wenigen Ausnahmen, die sie verlangt, doch die oben erwähnte Hauptschwierigkeit nicht gelöset. Denn falls diese Formel zur Berechnung des jüdischen Kalenders überhaupt angewandt werden soll, mufs man die Osterfeste in zwei nach einander folgenden Jahren bestimmen, um dadurch die Länge des verlangten Jahres zu berechnen. Dann mufs auch noch der Wochentag des Neujahrs, von welchem manche Fest- und Fasttage, da diese oft verschoben werden, abhängig sind, mit bestimmt werden.

In der That liefert die von Herrn Prof. *Nesselmann* im gegenwärtigen Journal mitgetheilte Abhandlung über den jüdischen Kalender, ungeachtet der sehr scharfsinnigen Entwicklung, den deutlichen Beweis von den auf diesem Gebiete sich findenden Schwierigkeiten.

Es verdient daher eine allgemeine Auflösung, welche sowohl nach der jüdischen als nach der christlichen Zeitrechnung bei jedem gegebenen Jahre

leicht und unmittelbar den ganzen Kalender des verlangten Jahres mit einemmale giebt, öffentlich mitgetheilt zu werden. Sie ist folgende.

Bekanntlich giebt es im jüdischen Kalender 14 verschiedene Jahresformeln oder Normalkalender, nach denen im ganzen Jahre sich die Festtage und andere damit zusammenhängende religiöse Gebräuche richten und die den Chronologen unter dem Namen Basch Gach etc. bekannt sind, welche Bezeichnungs-Art wir aber hier durch folgende ersetzen wollen:

$2k$, $2g$, $3m$, $5m$, $5g$, $7k$, $7g$ für die gemeinen Jahre,

$2K$, $2G$, $3M$, $5K$, $5G$, $7K$, $7G$ für die Schaltjahre.

In diesen Zeichen bedeuten die Zahlen die Wochentage, auf welche der Neujahrstag fällt; die Buchstaben k, g, m ein kurzes, ein grofses und ein mittleres Jahr, und zwar im gemeinen Jahre von 353, 355, 354, im Schaltjahre von 383, 385 und 384 Tagen. Dieses sind die beiden characteristischen Merkmale eines jeden Jahreskalenders. Dieses vorausgesetzt, läfst sich nun für die ganze jüdische Kalenderberechnung folgende allgemeine Aufgabe aufstellen.

I. Nach der jüdischen Zeitrechnung.

Bei jedem gegebenen Jahre A der jüdischen Zeitrechnung zu bestimmen, welcher von den 14 Normalkalendern in dem verlangten Jahre für einen vollkommenen Jahreskalender gelten soll.

Die Auflösung, welche also 14 verschiedene Fälle zu bestimmen hat, ist folgende:

Man dividire die Zahl $12A+7$ durch 19 und nenne den Rest R; ist dieser $=1$, so nehme man $19+1=R$. Man suche dann den Werth von

$$0{,}178117458.A+0{,}2220345.R+0{,}812684$$

und setze in der gefundenen Summe, die Ganzen unberücksichtigt, den Decimalbruch $=T$.

Das gesuchte Jahr A ist ein Schaltjahr, wenn $R<9$ gefunden wird; sonst aber immer ein gemeines Jahr. Der Kalender des Jahres A aber wird vermittels des gefundenen Werthes von T auf folgende Weise bestimmt.

Er ist nemlich:

Beim Schaltjahre =		Beim gemeinen Jahre =	
$2K$,	wenn $T=>0$,	$2k$,	wenn $T=>0$,
$2G$,	- - - - 0,157468,	$2g$,	- - - - 0,090410,
$3M$,	- - - - 0,285714,	$3m$,	- - - - 0,285714,
$5K$,	- - - 0,428571,	$5m$,	- - - - 0,376124,

Beim Schaltjahre =		Beim gemeinen Jahre =	
$5G$,	wenn $T = > 0{,}533570$,	$5g$,	wenn $T = > 0{,}661838$,
$7K$,	- - - - $0{,}714285$,	$7k$,	- - - - $0{,}714285$,
$7G$,	- - - - $0{,}871753$.	$7g$,	- - - - $0{,}804695$.

Ist im gemeinen Jahre der Werth von $R > 13$ bis 15 incl., so ändere man die Grenze bei $3m$ und setze dieselbe $= 0{,}271103$; ist R gröfser als 15, so ändere man aufserdem noch die Grenze bei $7g$ und setze an dessen Stelle $= 0{,}752248$.

Exempel. Man verlangt für das Jahr 5604 der jüdischen Zeitrechnung den ganzen Jahreskalender. Hier findet man $R = 14$, $T = 0{,}0914$. Das Jahr ist also ein gemeines Jahr und sein Jahreskalender $= 2g$, d. i. es fängt am Montag an, und seine Länge ist 355 Tage.

II. Nach der christlichen Zeitrechnung.

Bei jedem gegebenen Jahre A der christlichen Zeitrechnung zu finden, mit welchem Tage des christlichen Datums der jüdische Neujahrstag beginnt und welcher der 14 Normalkalender im ganzen Laufe dieses Jahres gebraucht werden soll.

Man dividire die Zahl $12A - 5$ durch 19 und nenne den Rest R, so dafs man, wenn sich $R = 1$ findet, $R = 1 + 19 = 20$ nimmt. Ferner dividire man A durch 4 und nenne den Rest r. Dann suche man die Zahl $25{,}98711 + 1{,}5542418 . R + 0{,}25 . r - 0{,}003177794 . A$ und nenne den Ausdruck $S + s$, so dafs S die ganze Zahl und s den Decimalbruch dieses Ausdrucks bezeichnen.

Endlich dividire man noch die Gröfse $(S + 3A + 5r)$ durch 7 und nenne den Rest T.

Das gesuchte Jahr ist ein Schaltjahr, wenn $R < 9$, ein gemeines aber, wenn $R = > 9$ ist. Der Kalender des gesuchten Jahres ist:

Im Schaltjahre =		Im gemeinen Jahre =	
$2K$,	wenn $(T + s) = > 0$ ist,	$2k$,	wenn $(T + s) = > 0$,
$2G$,	- - - - $1{,}10227$,	$2g$,	- - - - $0{,}63287$,
$3M$,	- - - - $2{,}0$,	$3m$,	- - - - $2{,}0$,
$5K$,	- - - - $3{,}0$,	$5m$,	- - - - $2{,}63287$,
$5G$,	- - - - $3{,}73514$,	$5g$,	- - - - $4{,}63287$,
$7K$,	- - - - $5{,}0$,	$7k$,	- - - - $5{,}0$,
$7G$,	- - - - $6{,}10227$.	$7g$,	- - - - $5{,}63287$.

Ist bei dem gemeinen Jahre $R > 13$ bis 15 incl., so ändere man bei dem Obigen die Grenze von $3m$ und setze dieselbe $= 1,89772$. Ist aber $R > 15$, so ändere man noch die Grenze von $7g$ und setze dieselbe $= 5,26574$.

Hat man den Kalender des gesuchten Jahres gefunden, und dessen Zahl sei z. B. $= d$, so beginnt dann der gesuchte Neujahrstag am $(S + d - T)$ten August alten Styls, oder wenn diese Gröfse gröfser als 31 ist, am $(S + d - T) - 31$ten September.

Exempel. Man suche den jüdischen Kalender für das Jahr 1847. Hier ist $R = 5$, $r = 3$, $T = 5$, $S + s = 28,65893$. Das gesuchte Jahr ist ein Schaltjahr, weil $R < 9$. Da aber $T + s > 5$, also der Kalender des laufenden Jahres $= 7K$ und $d = 7$ ist, so trifft der Neujahrstag auf den $(28 + 7 - 5) = 30$sten August alten Styls oder 11ten Sept. neuen Styls.

Das jüdische Jahr beginnt demnach am Sonnabend dem 11ten Sept., ist ein kurzes Schaltjahr von 383 Tagen, und von den 14 bekannten Kalendern ist das $7K$ genannte in dem laufenden Jahre für diesen Jahreskalender zu gebrauchen.

Einige Bemerkungen über die von Herrn Prof. *Nesselmann* in diesem Journal mitgetheilte Abhandlung über die Berechnung des jüdischen Kalenders.

Aufser einigen kleinen Erinnerungen gegen diese Abhandlung erfordern folgende Puncte eine nähere Beleuchtung.

Band 26. Seite 71 sagt Herr Prof. *Nesselmann*, dafs die Juden sich mit Unrecht der grofsen Genauigkeit und Kunstfertigkeit rühmen, die ihr Kalender habe, indem es im Laufe der Zeit bis dahin gekommen sei, dafs in den 3 Schaltjahren, welche die 8te, 11te und 19te Stelle im Cyklus einnehmen, ihr Passahfest nicht auf den ersten, sondern auf den zweiten Vollmond falle.

Hierüber ist Zweierlei zu bemerken:

1. Die Absicht, welche die jüdischen Chronologen bei der Begründung des Kalenders hatten, war nicht, wie manche Autoren glaubten, die, zu bewirken, dafs das Passahfest durchaus auf den 1ten Vollmond nach dem Frühlings-Aequinoctium falle, sondern nur, zu verhindern, dafs es nicht *vor* den 1ten Vollmond und nicht *nach* dem 2ten Vollmond fallen könne. Denn beliebig verschoben es erforderlichenfalls die Alten vom 1ten Vollmond auf den 2ten. Dies wird aus dem Pentateuch selbst entnommen, da der Unreine und der weit Abwesende das Passahfest am 2ten Monat feiern durften. Demnach kann es nicht, wie Herr Prof. *Nesselmann* sagt, als eine Abweichung oder Ver-

rückung angesehen werden, wenn das Passahfest einmal auf den 2ten Vollmond fällt; in welchem Falle es noch immer dem Haupt-Principe entspricht.

2. Scheint es nicht genau gerechnet zu sein, wenn Herr Prof. *Nesselmann* sagt, dafs die Verrückung schon 3mal den Cyklus trifft, nämlich beim 8ten, 11ten und 19ten; denn eigentlich findet derselbe nur beim 8ten und 19ten allein Statt, wenn man nur das wirklich mittlere astronomische Aequinoctium und den mittlern Vollmond rechnet. Der 11te aber wird seine Verrückung erst in 200 Jahren erhalten.

Beim Schlusse der Abhandlung wollte der Herr Prof. *Nesselmann* vermittels des jüdischen Kalenders den Todestag Christi suchen, welcher nach dem Evangelium auf den Freitag, den 13ten des jüdischen Monats Nissan fiel. Da aber dies mit der Berechnung des jüdischen Kalenders vor 1844 Jahren nicht stimmen wollte, so schliefst der Herr Verfasser daraus mit Evidenz, dafs die christliche Zeitrechnung, wie schon manche Critiker längst historisch bewiesen haben, nicht richtig sei, sondern dafs mit grofser Wahrscheinlichkeit der Todestag 5 Jahre früher gewesen sein mufs, indem damals der 13te Nissan auf den Freitag fiel. Es ist aber zu verwundern, dafs der Herr Verfasser, der mit der jüdischen Litteratur bekannt zu sein scheint, da er oft hie und da vom Talmud spricht, nicht berücksichtigt hat, dafs die Einrichtung des jüdischen Kalenders erst vom Jahre 500 n. Chr. an Statt findet. Selbst der Talmud soll noch gar keine feste Regeln zur Berechnung des Kalenders gehabt haben; und, wie verschiedene Stellen beweisen, hat der damalige Kalender gar nicht mit dem unsrigen übereingestimmt.

Endlich bemerkt Herr Prof. *Nesselmann*, dafs die von ihm in seiner Abhandlung aufgestellten Tafeln I. und II. schon 1842 in Königsberg von Herrn *Goldberg* besonders herausgegeben sind. Da sie aber ohne Erklärungen gedruckt worden seien, so könne er, trotz jener Schrift, seine Abhandlung für sein vollkommnes Eigenthum erklären. Es ist hier zu bemerken, dafs diese zwei oben gedachten sinnreichen Tafeln von Herrn *Goldberg* aus dem wohlbekannten chronologischen Werke Jefsod olam des Rabbi Isaac Israel zu Toledo 1310. ins Deutsche übertragen worden sind. Der Verfasser jenes Werks giebt diese Tafeln für eine alte Tradition aus. Dies zeigt, wie scharfsinnig die Entwicklung der Chronologie bei den Alten schon gewesen sei. Die Einrichtung der Tabellen ist in dem gedachten Werke zu sehen und daselbst auch zugleich die theoretische Entwicklung derselben zu finden.

15.

Allgemeine Bemerkungen über Rechenmaschinen, und Prospectus eines neu erfundenen Rechen-Instruments.

(Von Herrn *Ch. Z. Slonimsky* aus Bialystock in Rufsland.)

Jedem, der öfters grofse, zusammenhängende und mehrere Tage erfordernde Rechnungen auszuführen gehabt hat, ist bekannt, wie sehr anhaltendes Rechnen ermüdet und abstumpft; so dafs man öfter fehlt, ja bisweilen den Faden der Arbeit verliert und viele Umwege machen mufs. Besonders ist dies der Fall bei der Multiplication und Division vieler und so grofser Zahlen, dafs Logarithmen für dieselben nicht ausreichen. Die Producte der einzelnen Ziffern lassen sich zwar leicht aus dem Gedächtnisse finden, aber das im Sinnbehalten und Addiren der nicht hingeschriebenen Ziffern erfordert eine ununterbrochene genaue Aufmerksamkeit, und stets eine gewisse Anstrengung, welche, anhaltend fortgesetzt, sehr beschwerlich und abstumpfend ist. Die Möglichkeit von Fehlern, die bei der geringsten Unterbrechung der Aufmerksamkeit unterlaufen können, macht aber die ganze Rechnung mehr oder weniger *unsicher*. Noch mehr gilt Alles dies von der Division, indem man bei grofsen Divisionen oft erst versuchsweise verfahren mufs, ehe man den wahren Quotienten findet; so dafs bei so fortgesetzter ermüdender Arbeit leicht jedes bereits gefundene Resultat unsicher wird. Und wie peinlich ist es dann, die Rechnung Satz um Satz nochmals durchzusehen, um sich von der Richtigkeit des Resultats zu überzeugen.

Diesen Schwierigkeiten zu begegnen, haben schon früher Männer von grofser Gelehrsamkeit, selbst *Leibnitz*, Mühe und Kosten aufgewendet, um ein Werkzeug zu erfinden, mittels dessen man Rechnungsresultate erhalte, die immer fehlerfrei seien und welche die beim gewöhnlichen Rechnen erforderliche Aufmerksamkeit und das Kopfrechnen ganz oder zum Theil ersparen. *Leibnitz* soll, nächst einem Aufwande von mehr als 24 000 Thalern, viele seiner Nebenstunden mehrere Jahre lang dem Nachsinnen über diese Erfindung aufgeopfert haben. Der Pfarrer *Hahn* hat über seine Maschine 7 Jahre gearbeitet; Herr *Stern* in Warschau 8 Jahre, mit einem Aufwande von mehr als 10 000 Thlr.; und

neulich hat das Riesenwerk von *Babbage* in England 6 Jahre Zeit und einen Kosten-Aufwand von 17 000 Pfd. St. erfordert. Dergleichen künstliche Werkzeuge oder sogenannte Rechenmaschinen sind in der That zu verschiedenen Zeiten zu Tage gebracht worden; und mehreren glaubten ihre Erfinder einen so sichern Mechanismus und so viel Einfachheit gegeben zu haben, dafs sie sie für den allgemeinen Gebrauch passend hielten. Schon *Müller* soll für die von ihm im Jahr 1784 erfundene Rechenmaschine eine gröfsere Verbreitung gesucht haben. Allein bei aller Sicherheit und allen Vortheilen, die er bei derselben nachwies, gelang es ihm doch nicht, Theilnahme dafür zu gewinnen. Auch mehrere Gelehrte, die nach ihm die Rechenmaschinen vervollkommnet haben, versuchten vergebens, denselben allgemeinen Eingang zu verschaffen.

Die Ursach dieser Erfahrung, welche ich bei der von mir vor einigen Jahren erfundenen Maschine genauer erkannt habe, liegt nicht etwa in der Unvollkommenheit der Werkzeuge, sondern darin, dafs es schwer ist, den Rechnenden zu vermögen, seine Aufmerksamkeit, die er auf die gewöhnlichen Rechen-Operationen wenden mufs, in die behutsame Aufmerksamkeit auf die Manipulation einer Maschine zu verwandeln, und dann die Sicherheit beim Rechnen, ohne eigene Überzeugung, einem unsichtbaren, der Beschädigung ausgesetzten Räderwerke anzuvertrauen. In der That ist immer eine Verletzung oder Stockung bei einer Maschine zu besorgen, deren meisten Theile innerlich in ununterbrochener Bewegung getrieben werden, und die bald in bestimmten Puncten genau in einander greifen, bald wieder aufser Berührung kommen. Auch ist nicht, wie z. B. bei einer Uhr, die innere Beschädigung sogleich äufserlich sichtbar; vielmehr kann, da die Maschine selbst still steht, durch Bewegung der Kurbel sowohl ein falsches, als ein richtiges Resultat hervorgebracht werden.

Auch haben die mechanischen Rechenmaschinen noch den Mangel, dafs, wenn das Resultat erlangt ist, die Operation nicht mehr übersehen werden kann, um Überzeugung von deren Richtigkeit zu haben; wogegen man bei den gewöhnlichen Operationen mit der Feder noch immer wieder untersuchen kann, ob und wo ein Fehler sich eingeschlichen habe, den man dann sogleich zu verbessern im Stande ist. Mit der Maschine mufs man eines aus Unvorsichtigkeit begangenen Fehlers wegen die ganze Manipulation wiederholen. Besonders ist ein Fehler bei der Division leicht; so dafs sich behaupten läfst, es habe bis jetzt noch keine wirkliche Divisionsmaschine, selbst auf dem mechanischen Wege, gegeben. Denn da bei diesen Maschinen die Division in eine

Subtraction verwandelt werden soll, so mufs der Theil der Maschine, auf welcher der Divisor steht, unter die gehörigen Ziffern des Dividendus gebracht und von denselben so oftmal abgedreht werden, als die Subtraction möglich ist; und dann mufs wieder der bewegliche Theil um eine Stelle weiter gerückt und auf die nemliche Weise für jede Ziffer des Quotienten verfahren werden. Der Rechner mufs also bei jeder Umdrehung der Kurbel genau beobachten, ob der Dividendus nicht schon kleiner als der Divisor geworden ist. Hat er durch Versehen die Kurbel sogleich zu hemmen verfehlt, so ist seine ganze bisherige Rechnung vergeblich, und die Operation mufs von neuem gemacht werden. Bei meiner *mechanischen* Rechenmaschine ist dies schon der Fall nicht; weil die Kurbel, sammt dem Räderwerk, sowohl rechts, bei der Addition und Multiplication, als bei der Subtraction und Division links gedreht werden kann, und also bei jedem begangenen Fehler die ersten Ziffern zurückgebracht werden können; welches besonders für die Division, für die Regel de tri und andere zusammenhängende Rechnungen von Nutzen ist.

Es ist auf solche Weise leicht zu sehen, weshalb mechanische Rechenmaschinen keinen Eingang finden. Abgesehen von ihrer grofsen Kostspieligkeit und der nöthigen vorsichtigen Aufmerksamkeit auf ihre Handhabung, damit weder die Maschine, noch die Rechnung leide, wird man auch bei einem für zuverlässig gehaltenen Instrumente Rechnungen, die man oft dem Kopfrechner nicht zutraute, nicht einem Mechanismus anvertrauen wollen, von dessen innerem guten Zustande und von dessen richtigem Gebrauch, ja selbst, ob beim Anfange der Rechnung keine fremde Zahl in der Maschine gewesen sei, man sich nur vermittels des gewöhnlichen Nachrechnens zu überzeugen im Stande ist.

Man hat sich deshalb auch um *tabellarische* Hülfsmittel bemüht; das heifst, um Mittel, die ihren Grund in bereits fertig ausgerechneten Zahlen haben, und durch welche gewissermafsen vermittels der vor unsern Augen geschehenden Operationen das verlangte Resultat gefunden wird. Solche Tafeln sind zwar in Hinsicht ihrer Einfachheit zuverlässiger als die *mechanischen* Rechenmaschinen, aber mit allen bisherigen Versuchen dieser Art ist man noch nicht dahin gekommen, dem Rechner dadurch eine wesentliche Erleichterung zu verschaffen. Die einzige und vorzüglichste Erleichterung für Multiplicationen und Divisionen würde sein, wenn man im Stande wäre, vermittels irgend einer sichern und verläfslichen Operation von *jeder vielziffrigen Zahl* die 2, 3, 4, 5, 6, 7, 8 und 9fachen gleich mit einemmale zu erhalten. Dann hätte man für eine Multiplication nur eine Addition und für eine Division nur eine Subtraction zu machen. Verlangte

man z. B. die Zahl 73948 mit 8967 zu multipliciren, so würde man, da die 8 einfachen Producte der Zahl, nemlich das 2, 3, 4, 5, 6, 7, 8 und 9fache von 73948 schon ausgerechnet sind, von denselben nur die Producte mit 7, 6, 9 und 8 unter einander, jedes um eine Stelle links gerückt, abzuschreiben und zu addiren haben; welche Summe dann das verlangte Product geben würde. Bei der Division wäre umgekehrt zu verfahren; nemlich, wenn man immer von den 8 einfachen Producten des Divisors dasjenige, welches das nächste zu den letzten Ziffern des Dividendus ist, von demselben subtrahirte, so bekäme man nach und nach alle Ziffern des Quotienten. Man ersparte also so bei der Multiplication das Multipliciren, bei der Division aber das probirte Dividiren, und nachher bei jeder gefundenen Ziffer des Quotienten das Multipiciren.

Aber diesen Zweck auf dem sichersten Wege zu erreichen, nemlich von jeder vielziffrigen Zahl ihre 8 einfachen Producte unmittelbar mit einemmale darzustellen, ist durch alle bisherigen Versuche noch nicht gelungen. Die bekannten Neperschen Stäbe, oder die aus denselben zusammengesetzten Maschinen von *Caspar Wolf*, geben nicht die 8 einfachen Producte jeder beliebigen Zahl vollständig, sondern man mufs noch bei jedem einzelnen Producte die Zehner jeder multiplicirten Ziffer zu den nachfolgenden Einern in Gedanken addiren; und die Zehner und Einer stehen überdies in einer ungeschickten Stellung; nemlich in einer Reihe nach einander vermengt, welches beim Addiren genaue Aufmerksamkeit erfordert und für die Multiplication unbequem und dadurch unsicher, zur Division aber gar nicht anwendbar ist, weil sich nicht die Reihe der Zahlen erkennen läfst, welche nach ihrer Zusammen-Addirung der Zehner mit den nachfolgenden Einern die nächste zum Dividendus ist.

Selbst die bekannten Multiplicationstabellen, welche, bis zu einer gewissen Zahl, von jeder Zahl ihre 8 einfachen Producte unmittelbar anzugeben bestimmt sind, konnten den verlangten Zweck nicht erfüllen. Abgesehen von der Unsicherheit derselben, da für die Correctur von Bänden starken Zahlentafeln keine Bürgschaft Statt findet, geben sie auch nicht von jeder vielziffrigen Zahl die verlangten 8 Producte unmittelbar, sondern man mufs die Ziffern jedes verlangten Products von verschiedenen Stellen her zusammenlesen und nach einer gewissen Ordnung abschreiben; welches bei der Multiplication Geduld und Vorsicht verlangt, bei der Division aber, weil sich nicht alle 8 Producte des Divisors mit einem Blicke übersehen lassen, um unter ihnen das nächste am Dividendus herauszufinden, unanwendbar ist. Sollen dagegen solche Tabellen bis zu einer 7ziffrigen Zahl vollständig sein, so dafs sie von jeder Zahl alle 8 einfachen

Producte ohne weiteres geben, so erfordert dieses, wie Herr *Crelle* zu seinen Tafeln bemerkt hat, 117 Quartbände, jeden von 127 Bogen stark.

Dieses Alles erwogen, erlaube ich mir, ein neues, von mir erfundenes Rechen-Instrument, welches an Einfachheit, Sicherheit und Zuverlässigkeit vor den oben gedachten Maschinen sich auszeichnen dürfte, hiermit den Sachkennern und den Rechnern zu empfehlen.

Dasselbe besteht aus einem hölzernen Kästchen von 14 Zoll lang, 10 Zoll breit und $2\frac{1}{4}$ Zoll hoch, welches von jeder, bis auf 7 Stellen beliebigen Zahl, die auf dem Kästchen mittels einer leichten Operation aufgestellt wird, alle 8 einfachen Producte, nämlich das 2, 3, 4, 5, 6, 7, 8 und 9fache, unmittelbar in 8 untereinander geordneten Reihen vollständig giebt, so dafs für jede Multiplication nur eine Addition und für jede Division nur eine Subtraction zu machen bleibt.

Mittels einer andern einfachen Operation mit diesem Instrumente läfst sich auch jede beliebige Quadratwurzel ausziehen. Die Wurzel der 2 ersten Ziffern jedes Quadrats giebt das Instrument unmittelbar. Stellt man das 2fache der gefundenen Wurzel auf, sie sei z. B. gleich a, so giebt das Instrument die 2 übrigen Glieder, nemlich $2ab+b^2$ für jeden Werth von b, von 1 bis 9. Man darf dann nur das dieser Columne des Quadrats nächste Product von derselben subtrahiren und mit dem gebliebenen Rest auf die nämliche Weise u. s. w. verfahren, so findet man nach einander alle Ziffern der Wurzel. Es werden also so die beschwerlichsten Operationen bei jeder Ausziehung der Quadratwurzel, nemlich die Versuche, um die richtige Wurzel zu treffen und nachher mit derslben das Glied $2a+b$ zu multipliciren, erspart.

Die Vorzüge des Instruments vor den bis jetzt bekannten Hülfsmitteln sind einleuchtend. Bei den gewöhnlichen *mechanischen* Rechenmaschinen, wenn sie auch alle Additionen und Subtractionen verrichten, wiegen die Vortheile die vielen oben bemerkten Nachtheile nicht auf; die sie vielmehr zum allgemeinen Gebrauch ungeschickt machen. Dagegen hat das Instrument vor den *mechanischen* Mitteln folgende Vorzüge.

1. Es ist *zuverlässig*, weil es seine Resultate *nicht* auf mechanischem Wege hervorbringt, nemlich *nicht* durch Bewegung. Es beruht vielmehr auf einem besondern Zahlentheorem. Ich habe dieses Theorem Herrn *Crelle* mitgetheilt, und er hat einen allgemeinen Beweis davon gefunden. Der kleine Mechanismus des Instruments nimmt an den Berechnungen gar keinen Antheil, sondern ist blofs da, um die für die Anwendung des Theorems erforderliche

Manipulation schnell und leicht hervorzubringen. Ist dieselbe hervorgebracht, so liegt die Richtigkeit des Resultats dem Rechner deutlich vor Augen, ohne weiter dem Mechanismus im geringsten vertrauen zu dürfen, während man bei den mechanischen Rechenmaschinen sich blindlings auf verborgene und complicirte Mechanismen verlassen mufs.

2. Bei jedem Resultat bleibt sowohl die erste aufgestellte Zahl, als die ganze Operation noch sichtbar, so dafs der Rechner mit einem Überblick von der Richtigkeit des Geschehenen sich überzeugen kann; auch wenn er die Operation durch Jemand Andern hat verrichten lassen. Hat irgend ein Fehler bei der Operation Statt gefunden, so wird er deutlich bemerkt und ist leicht abzustellen; während bei den mechanischen Rechenmaschinen, weil die Operationen selbst ganz verschwinden, ein begangener Fehler nicht zu bemerken und, wenn man ihn auch kennte, nicht mehr zu verbessern ist.

3. Die Maschine bietet ihrer Construction nach, denn sie ist aus gleichen, massiven, mehrentheils hölzernen Theilen zusammengesetzt, deren Zusammenstellung und Bewegung höchst einfach ist, die gröfste Sicherheit dar. Sie kann fast nie Schaden leiden; und wenn es auf irgend eine Weise geschehen sollte, so ist der Schaden äufserlich sichtbar und leicht wegzuschaffen.

4. Will man vermittels dieser Maschine mit Multiplicatoren, Divisoren und Wurzeln rechnen, die mehr als 7 Stellen haben, so braucht man nur zwei Exemplare der Maschine neben einander zu setzen; diese beiden geben dann mittels einer kleinen Operation, gleich einer einzelnen Maschine, Zahlen von 12 Stellen. Überhaupt läfst sich durch n nebeneinander gestellte 7ziffrige Maschinen eine Maschine für Zahlen von $6n+1$ Ziffern herstellen.

5. Da die Maschine sehr einfach ist, so läfst sie sich von gewöhnlichen Arbeitern verfertigen und ist verhältnifsmäfsig sehr wohlfeil; sie kann, fabrikmäfsig verfertigt, höchstens 6 bis 7 Thlr. kosten.

Eine solche Maschine habe ich während meines kurzen Aufenthalts in Berlin verfertigen lassen und auch der Akademie der Wissenschaften in ihrer Sitzung vom 8ten August vorgezeigt.

Bemerkung des Herausgebers dieses Journals. Der Herr Verfasser der vorstehenden Abhandlung erwähnt in derselben, ich habe bei meinen Rechentafeln geäufsert, die 2, 3, 4, 5, 6, 7, 8 und 9fachen aller 7ziffrigen Zahlen vollständig zu drucken, würden 117 Quartbände jeder von 127 Bogen nöthig

sein. Dem ist allerdings so: aber ich habe auch durch die That, nemlich durch eben jene Tafeln, bewiesen, dafs sich die genannten Producte auch in *einen einzigen* Band von 125 Bogen bringen lassen. Die Producte stehen hier freilich nicht jedes in einer und derselben Zeile, aber sie sind recht gut eines neben dem andern zu übersehen. Auch meine frühern, in Octav gedruckten Rechentafeln vom Jahr 1820, welche die 2, 3, 4 bis 1000fachen der Zahlen von 1 bis 1000 angeben, würden nur *einen* Quartband füllen. Gegen die Rechentafeln, als Hülfsmittel beim Rechnen, dürfte also wohl *der* Einwand, dafs sie zu *voluminös* sind, nicht Statt finden. Auch dafs bei dem Druck Fehler entstehen können, dürfte kein Einwand sein: denn die Druckfehler finden sich, wenn die Correctur, wie es geschehen mufs, *rechnend* gemacht wird, fast ohne Ausnahme; und die dennoch etwa bleibenden wenigen Fehler finden sich beim Gebrauch der Tafeln allmälig; und sind sie alle gefunden, und werden dann die Tafeln stereotypirt, so sind *diese* für immer fehlerfrei.

Ich will es indessen gern zugeben, dafs eine gut ausgedachte, und besonders eine recht *einfache* Rechenmaschine, vielen Rechnern angenehmer sein wird, als irgend eine gedruckte Rechentafel. Eine solche *gute* Rechenmaschine scheint mir, von den beiden, vom Herrn Verfasser aufgestellten, besonders die zweite, hier oben beschriebene zu sein. Herr *Slonimsky* hat die Güte gehabt, mir seine beiden Maschinen und ihren Gebrauch zu zeigen. Beide sind nach meiner Meinung ungemein sinnreich, und die zweite ist höchst einfach.

Das Zahlentheorem, auf welchem, wie der Herr Verfasser in der Abhandlung bemerkt, die zweite Maschine beruht, ist ebenfalls recht interessant; ich werde es, nebst dem Beweise desselben, auf welchen ich gekommen bin, bekannt machen, sobald der Herr Verfasser über seine Maschine verfügt haben wird.

16.

Aufgaben.

---

1. Von Herrn Stud. *Eisenstein.*

Die beiden Producte

$$(1+x\sin\varphi)(1+x\sin 2\varphi)(1+x\sin 3\varphi)\dots(1+x\sin n\varphi),$$
$$(1+x\cos\varphi)(1+x\cos 2\varphi)(1+x\cos 3\varphi)\dots(1+x\cos n\varphi)$$

nach Potenzen von x zu entwickeln.

2. Von Andern.

Wenn man aus den m^2 Factoren

$$\begin{array}{l} a_1,\ b_1,\ c_1,\ d_1,\ \dots\ m_1;\\ a_2,\ b_2,\ c_2,\ d_2,\ \dots\ m_2;\\ a_3,\ b_3,\ c_3,\ d_3,\ \dots\ m_3;\\ \dots\dots\dots\dots\\ a_m,\ b_m,\ c_m,\ d_m,\ \dots\ m_m \end{array}$$

alle möglichen Producte, jedes von m Factoren, unter der Bedingung aufstellt, dafs in keinem Product mehr als ein a, ein b, ein c etc. und auch kein Zeiger der $a, b, c \dots$ mehr als einmal vorkomme, so also, dafs z. B. für die $3^2=9$ Gröfsen

$$\begin{array}{l} a_1,\ b_1,\ c_1,\\ a_2,\ b_2,\ c_2,\\ a_3,\ b_3,\ c_3 \end{array}$$

die Producte folgende wären:

$$a_1b_2c_3,\quad a_1b_3c_2,\quad a_2b_1c_3,\quad a_2b_3c_1,\quad a_3b_1c_2,\quad a_3b_2c_1,$$

so ist die *Anzahl* der auf diese Weise möglichen Producte bekanntlich

$$= 1.2.3.4.5\dots m.$$

Welche ist nun die Zahl der Producte, die *übrig* bleiben, wenn *bestimmte a, bestimmte b, c, d* etc. *gleich Null* sind? Z. B., welches ist die Zahl der Producte obiger Art, jedes von 8 Factoren, aus den 64 Gröfsen

$$\begin{array}{l}
a_1,\ b_1,\ c_1,\ d_1,\ e_1,\ f_1,\ g_1,\ h_1, \\
a_2,\ b_2,\ c_2,\ d_2,\ e_2,\ f_2,\ g_2,\ h_2, \\
a_3,\ b_3,\ c_3,\ d_3,\ e_3,\ f_3,\ g_3,\ h_3, \\
a_4,\ b_4,\ c_4,\ d_4,\ e_4,\ f_4,\ g_4,\ h_4, \\
a_5,\ b_5,\ c_5,\ d_5,\ e_5,\ f_5,\ g_5,\ h_5, \\
a_6,\ b_6,\ c_6,\ d_6,\ e_6,\ f_6,\ g_6,\ h_6, \\
a_7,\ b_7,\ c_7,\ d_7,\ e_7,\ f_7,\ g_7,\ h_7, \\
a_8,\ b_8,\ c_8,\ d_8,\ e_8,\ f_8,\ g_8,\ h_8,
\end{array}$$

wenn

$$\left.\begin{array}{l}
a_6,\ b_7,\ c_1,\ d_1,\ e_7,\ f_1,\ g_1,\ h_1 \\
a_7,\ b_8,\ c_8,\ d_2,\ e_8,\ f_8,\ g_2,\ h_2 \\
a_8 \qquad\quad \text{und} \qquad\quad h_3
\end{array}\right\} = 0 \text{ sind?}$$

Druckfehler.

Im 26ten Bande S. 186 Z. 11 v. o. lese man

bei jener ein Rotations-Ellipsoïd, ein Rotations-Hyperboloïd und einen der Länge entsprechenden Winkel einführt;

anstatt

bei jener mit einem Rotations-Ellipsoïd, einem Rotations-Hyperboloïd und einem der Länge entsprechenden Winkel ausreicht;

Im 27ten Bande S. 358 Z. 7 und 6 v. u. müssen die Worte

und mithin, da nach $(a.)$ jedes $p-r$ einem r gleich ist, auch kein $p-\varrho$ einem r

und Z. 4. v. u. die Worte

jedes $p-\varrho$ einem ϱ gleich. Das heifst:

wegfallen.

ullischen

sweise, aber
en Bernoulli-
lung der hö-
welches ich,
der auf die-
dern Mathe-
ung gehörig
wiederholen.
en, habe ich
tze den von
en und die
eit es ohne

Reihe

$\cdot x^n$,
n Potenzen
$= 0$

önnen, hat

$$S(x, n) = 1^n + 2^n + 3^n + \ldots + y^n + \ldots + x^n$$

wenn

Im 26te

Im 27ten

17.

Entwicklung der Functionsweise der Bernoullischen Zahlen.

(Von Herrn Dr. *O. Eisenlohe* zu Carlsruhe.)

---

§. 1.

Soviel mir bekannt, hat man zwar die zurücklaufende Bildungsweise, aber bis jetzt noch nicht die eigentliche Functionsweise der sogenannten Bernoullischen Zahlen gefunden; jedoch kann diese Aufgabe ohne Anwendung der höhern Analysis durch ein eigenthümliches Verfahren gelöset werden, welches ich, da es mir nicht unwichtig scheint, hier mittheilen will. Ein Theil der auf diesem Wege von mir erhaltenen Resultate ist zwar schon von andern Mathematikern angegeben worden; um aber die vollständige Entwicklung gehörig auffassen zu können, ist es nothwendig, diese Angaben hier zu wiederholen.

Um diesem Aufsatze keine allzugrofse Ausdehnung zu geben, habe ich mich genöthigt gesehen, bei der Entwicklung der einzelnen Gesetze den von mir eingeschlagenen Weg meistens nur im Allgemeinen anzudeuten und die oft sehr weitläufigen besondern Umformungen wegzulassen, insoweit es ohne der Deutlichkeit Eintrag zu thun geschehen konnte.

I. Umformung der Reihe $1^n+2^n+3^n+\dots+x^n$ in eine Reihe nach den Potenzen von x.

§. 2.

Setzt man zur Abkürzung

1. $$S(x,n) = 1^n+2^n+3^n+\dots+y^n+\dots+(x-1)^n+x^n,$$

so kann diese Reihe umgeformt und durch eine andere, nach den Potenzen von x geordnete Reihe dargestellt werden. Es ist nämlich für $n=0$

$$S(x,0) = 1^0+2^0+3^0+\dots+x^0 = x$$

und für $n=1$

$$S(x,1) = 1+2+3+\dots+x = \tfrac{1}{2}x(x+1).$$

Um aber für höhere Werthe von n die Umformung ausführen zu können, hat man zu berücksichtigen, dafs, wenn

$$S(x,n) = 1^n+2^n+3^n+\dots+y^n+\dots+x^n$$

gesetzt wird, die Reihe

$$y^n+(y+1)^n+\ldots+x^n = S(x,n)-S(y-1,n)$$

gesetzt werden kann. Man erhält nun, wenn $n-1$ statt n gesetzt wird,

$$S(x,n-1) = 1^{n-1}+2^{n-1}+3^{n-1}+\ldots+y^{n-1}+\ldots+x^{n-1};$$

also

$$1^{n-1}+2^{n-1}+3^{n-1}+\ldots+y^{n-1}+\ldots+(x-1)^{n-1}+x^{n-1}=S(x,n-1),$$
$$2^{n-1}+3^{n-1}+\ldots+y^{n-1}+\ldots+(x-1)^{n-1}+x^{n-1}=S(x,n-1)-S(1,n-1),$$
$$3^{n-1}+\ldots+y^{n-1}+\ldots+(x-1)^{n-1}+x^{n-1}=S(x,n-1)-S(2,n-1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$y^{n-1}+\ldots+(x-1)^{n-1}+x^{n-1}=S(x,n-1)-S(y-1,n-1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(x-1)^{n-1}+x^{n-1}=S(x,n-1)-S(x-2,n-1),$$
$$x^{n-1}=S(x,n-1)-S(x-1,n-1).$$

Werden diese Reihen zusammengezählt, so ergiebt sich

$$1^n+2^n+3^n+\ldots+y^n+\ldots+(x-1)^n+x^n$$
$$=x.S(x,n-1)-S(1,n-1)-S(2,n-1)-\ldots-S(y,n-1)-\ldots-S(x-1,n-1),$$

oder

$$2.\quad S(x,n) = x.S(x,n-1)-\Sigma y.S(y,n-1),\quad y=1,2,3,\ldots,(x-1);$$

wo das Zeichen Σy bedeutet, dafs dem y alle ganzen Zahlenwerthe von 1 bis und einschliefslich $x-1$ gegeben werden sollen.

Dieser Ausdruck giebt die zurücklaufende Bildungsweise für $S(x,n)$ und kann auf verschiedenen Wegen zur unabhängigen Bildungsweise führen, von welchen Wegen der einfachste der ist, wenn man die Reihen, welche für mehrere Zahlenwerthe von n entstehen, zusammenstellt, indem sich alsdann das Gesetz der Bildungsweise hieraus leicht ergiebt.

Man erhält z. B. für $n=2$

$$S(x,2)=x.S(x,1)-S(1,1)-S(2,1)-\ldots-S(y,1)-\ldots-S(x-1,1).$$

Nun ist aber

$$S(x,1) = x.\frac{x+1}{2} = \frac{x^{2|1}}{1^{2|1}},\qquad S(y,1) = y.\frac{y+1}{2} = \frac{y^{2|1}}{1^{2|1}},$$

daher wird

$$S(x,2) = x.\frac{x^{2|1}}{1^{2|1}}-\frac{1^{2|1}}{1^{2|1}}-\frac{2^{2|1}}{1^{2|1}}-\ldots-\frac{y^{2|1}}{1^{2|1}}-\ldots-\frac{(x-1)^{2|1}}{1^{2|1}}$$
$$= x.\frac{x^{2|1}}{1^{2|1}}-\frac{(x-1)^{3|1}}{1^{3|1}}$$
$$= x.\frac{x.(x+1)(2x+1)}{1^{3|1}} = \frac{x^3}{3}+\frac{x^2}{2}+\frac{x}{6}.$$

Man findet auf diese Weise

$$S(x,0) = x,$$

$$S(x,1) = \frac{x^2}{2} + \frac{x}{2},$$

$$S(x,2) = \frac{x^3}{3} + \frac{x^2}{2} + 2.\frac{x}{12},$$

$$S(x,3) = \frac{x^4}{4} + \frac{x^3}{2} + 3.\frac{x^2}{12},$$

$$S(x,4) = \frac{x^5}{5} + \frac{x^4}{2} + 4.\frac{x^3}{12} - \frac{4^{3|-1}}{1^{3|1}}.\frac{x}{120},$$

$$S(x,5) = \frac{x^6}{6} + \frac{x^5}{2} + 5.\frac{x^4}{12} - \frac{5^{3|-1}}{1^{3|1}}.\frac{x^2}{120},$$

$$S(x,6) = \frac{x^7}{7} + \frac{x^6}{2} + 6.\frac{x^5}{12} - \frac{6^{3|-1}}{1^{3|1}}.\frac{x^3}{120} + \frac{6^{5|-1}}{1^{5|1}}.\frac{x}{252},$$

$$S(x,7) = \frac{x^8}{8} + \frac{x^7}{2} + 7.\frac{x^6}{12} - \frac{7^{3|-1}}{1^{3|1}}.\frac{x^4}{120} + \frac{7^{5|-1}}{1^{5|1}}.\frac{x^2}{252}$$

u. s. w.,

$$S(x,20) = \frac{x^{21}}{21} + \frac{x^{20}}{2} + \frac{20^{1|-1}}{1^{1|1}}.\frac{x^{19}}{12} - \frac{20^{3|-1}}{1^{3|1}}.\frac{x^{17}}{120} + \frac{20^{5|-1}}{1^{5|1}}.\frac{x^{15}}{252} - \frac{20^{7|-1}}{1^{7|1}}.\frac{x^{13}}{240}$$
$$+ \frac{20^{9|-1}}{1^{9|1}}.\frac{x^{11}}{132} - \frac{20^{11|-1}}{1^{11|-1}}.x^9.\frac{691}{32760} + \frac{20^{13|-1}}{1^{13|1}}.\frac{x^7}{12} - \frac{20^{15|-1}}{1^{15|1}}.x^5.\frac{3617}{8160}$$
$$+ \frac{20^{17|-1}}{1^{17|1}}.x^3.\frac{43867}{14364} - \frac{20^{19|-1}}{1^{19|1}}.x.\frac{174611}{6600},$$

$$S(x,21) = \frac{x^{22}}{22} + \frac{x^{21}}{2} + \frac{21^{1|-1}}{1^{1|1}}.\frac{x^{20}}{12} - \frac{21^{3|-1}}{1^{3|1}}.\frac{x^{18}}{120} + \frac{21^{5|-1}}{1^{5|1}}.\frac{x^{16}}{252} - \frac{21^{7|-1}}{1^{7|1}}.\frac{x^{14}}{240}$$
$$+ \frac{21^{9|-1}}{1^{9|1}}.\frac{x^{12}}{132} - \frac{21^{11|-1}}{1^{11|1}}.x^{10}.\frac{691}{32760} + \frac{21^{13|-1}}{1^{13|1}}.\frac{x^8}{12} - \frac{21^{15|-1}}{1^{15|1}}.x^6.\frac{3617}{8160}$$
$$+ \frac{21^{17|-1}}{1^{17|1}}.x^4.\frac{43867}{14364} - \frac{21^{19|-1}}{1^{19|1}}.x^2.\frac{174611}{6600}.$$

In diesen Reihen treten als Coëfficienten der einzelnen Glieder gewisse Zahlen auf, welche nach ihrem Entdecker *Jacob Bernoulli* die *Bernoullischen Zahlen* heifsen, und deren Bildungsweise noch unbekannt ist. Die Bezeichnung derselben ist folgende:

$$\mathfrak{B}_1 = 2.\frac{1}{12} = \frac{1}{6}, \qquad \mathfrak{B}_{11} = 12.\frac{691}{32760} = \frac{691}{2730},$$

$$\mathfrak{B}_3 = 4.\frac{1}{120} = \frac{1}{30}, \qquad \mathfrak{B}_{13} = 14.\frac{1}{12} = \frac{7}{6},$$

$$\mathfrak{B}_5 = 6.\frac{1}{252} = \frac{1}{42}, \qquad \mathfrak{B}_{15} = 16.\frac{3617}{8160} = \frac{3617}{510},$$

$$\mathfrak{B}_7 = 8.\frac{1}{240} = \frac{1}{30}, \qquad \mathfrak{B}_{17} = 18.\frac{43867}{14364} = \frac{43867}{798},$$

$$\mathfrak{B}_9 = 10.\frac{1}{132} = \frac{5}{66}, \qquad \mathfrak{B}_{19} = 20.\frac{174611}{6600} = \frac{174611}{330}$$

u. s. w.

Führt man diese Bezeichnung statt der Zahlencoëfficienten in die Reihe ein, und bemerkt, dafs die Bildungsweise von $S(x,n)$ für ein gerades und für ein ungerades n verschieden ist, so erhält man allgemein

3. $S(x, 2n)$

$$= \frac{x^{2n+1}}{2n+1} + \frac{x^{2n}}{2} + \frac{(2n)^{1|-1}}{1^{1|1}} \cdot \frac{\mathfrak{B}_1}{2} \cdot x^{2n-1} - \frac{(2n)^{3|-1}}{1^{3|1}} \cdot \frac{\mathfrak{B}_3}{4} \cdot x^{2n-3}$$
$$+ \frac{(2n)^{5|-1}}{1^{5|1}} \cdot \frac{\mathfrak{B}_5}{6} \cdot x^{2n-5} - + \dots (-)^m \cdot \frac{(2n)^{2m+1|-1}}{1^{2m+1|1}} \cdot \frac{\mathfrak{B}_{2m+1}}{2m+2} \cdot x^{2n-2m-1} + - \dots$$
$$(-)^{n-2} \cdot \frac{(2n)^{2n-3|-1}}{1^{2n-3|1}} \cdot \frac{\mathfrak{B}_{2n-3}}{2n-2} \cdot x^3 + (-)^{n-1} \cdot \frac{(2n)^{2n-1|-1}}{1^{2n-1|1}} \cdot \frac{\mathfrak{B}_{2n-1}}{2n} \cdot x^1$$

und

4. $S(x, 2n+1)$

$$= \frac{x^{2n+2}}{2n+2} + \frac{x^{2n+1}}{2} + \frac{(2n+1)^{1|-1}}{1^{1|1}} \cdot \frac{\mathfrak{B}_1}{2} \cdot x^{2n} - \frac{(2n+1)^{3|-1}}{1^{3|1}} \cdot \frac{\mathfrak{B}_3}{4} \cdot x^{2n-2}$$
$$+ \frac{(2n+1)^{5|-1}}{1^{5|1}} \cdot \frac{\mathfrak{B}_5}{6} \cdot x^{2n-4} - + \dots (-)^m \cdot \frac{(2n+1)^{2m+1|-1}}{1^{2m+1|1}} \cdot \frac{\mathfrak{B}_{2m+1}}{2m+2} \cdot x^{2n-2m} + - \dots$$
$$(-)^{n-2} \cdot \frac{(2n+1)^{2n-3|-1}}{1^{2n-3|1}} \cdot \frac{\mathfrak{B}_{2n-3}}{2n-2} \cdot x^4 + (-)^{n-1} \cdot \frac{(2n+1)^{2n-1|-1}}{1^{2n-1|1}} \cdot \frac{\mathfrak{B}_{2n-1}}{2n} \cdot x^2.$$

In diesen Gleichungen bedeutet (für $p = 2n$ und $p = 2n+1$)

$$S(x,p) = 1^p + 2^p + 3^p + \dots + x^p,$$
$$\mathfrak{B}_{2m+1} = \text{die } (m+1)\text{te Bernoullische Zahl und}$$
$$\frac{p^{2m+1|-1}}{1^{2m+1|1}} = \frac{p.(p-1).(p-2) \times \dots \times (p-2m)}{1.2.3 \times \dots \times (2m).(2m+1)}.$$

Diese beiden Formeln geben das Gesetz an, nach welchem die durch $S(x,n)$ bezeichnete Reihe in eine andere nach den Potenzen von x geordnete Reihe umgeformt werden kann. Da aber die Bildungsweise der darin als Coëfficienten auftretenden Bernoullischen Zahlen unbekannt ist, so hat man diese noch zu suchen. Zur Lösung dieser Aufgabe können zwei verschiedene Wege eingeschlagen werden, auf welchen man sowohl die zurücklaufende als auch die unabhängige Bildungsweise für $\mathfrak{B}_{2m+1}$ erhält.

II. Aufsuchung der zurücklaufenden Bildungsweise der Bernoullischen Zahlen.

§. 3.

Aus den Gleichungen 3. und 4. kann die zurücklaufende Bildungsweise für $\mathfrak{B}_{2n-1}$ leicht gefunden werden. Da nämlich beide Gleichungen für jeden Werth von x gelten müssen, und für $x = 1$, wo

$$S(x,2n)=1, \qquad S(x,2n+1)=1$$

ist, die Potenzen von x wegfallen, so erhält man aus Gl. 3.

$$1=\frac{1}{2n+1}+\frac{1}{2}+\frac{(2n)^{1|-1}}{1^{1|1}}\cdot\frac{\mathfrak{B}_1}{2}-\frac{(2n)^{3|-1}}{1^{3|1}}\cdot\frac{\mathfrak{B}_3}{4}+\frac{(2n)^{5|-1}}{1^{5|1}}\cdot\frac{\mathfrak{B}_5}{6}-+\dots$$

$$(-)^p.\frac{(2n)^{2p+1|-1}}{1^{2p+1|1}}\cdot\frac{\mathfrak{B}_{2p+1}}{2p+2}-+\dots(-)^{n-2}.\frac{(2n)^{2n-3|-1}}{1^{2n-3|1}}\cdot\frac{\mathfrak{B}_{2n-3}}{2n-2}+(-)^{n-1}.\frac{(2n)^{2n-1|-1}}{1^{2n-1|1}}\cdot\frac{\mathfrak{B}_{2n-1}}{2n},$$

oder

$$5. \quad (-)^n\mathfrak{B}_{2n-1}=-\frac{2n-1}{2.(2n+1)}+\frac{(2n)^{1|-1}}{1^{1|1}}\cdot\frac{\mathfrak{B}_1}{2}-\frac{(2n)^{3|-1}}{1^{3|1}}\cdot\frac{\mathfrak{B}_3}{4}+\frac{(2n)^{5|-1}}{1^{5|1}}\cdot\frac{\mathfrak{B}_5}{6}-+.$$

$$(-)^p.\frac{(2n)^{2p+1|-1}}{1^{2p+1|1}}\cdot\frac{\mathfrak{B}_{2p+1}}{2p+2}+-\dots(-)^{n-2}.\frac{(2n)^{2n-3|-1}}{1^{2n-3|1}}\cdot\frac{\mathfrak{B}_{2n-3}}{2n-2}.$$

Und ebenso erhält man aus Gl. 4.

$$6. \quad 0=-\frac{n}{2n+2}+\frac{(2n+1)^{1|-1}}{1^{1|1}}\cdot\frac{\mathfrak{B}_1}{2}-\frac{(2n+1)^{3|-1}}{1^{3|1}}\cdot\frac{\mathfrak{B}_3}{4}+\frac{(2n+5)^{5|-1}}{1^{5|1}}\cdot\frac{\mathfrak{B}_5}{6}-+\dots$$

$$(-)^p.\frac{(2n+1)^{2p+1|-1}}{1^{2p+1|1}}\cdot\frac{\mathfrak{B}_{2p+1}}{2p+2}-+\dots(-)^{n-2}.\frac{(2n+1)^{2n-3|-1}}{1^{2n-3|1}}\cdot\frac{\mathfrak{B}_{2n-3}}{2n-2}$$

$$+(-)^{n-1}.\frac{(2n+1)^{2n-1|-1}}{1^{2n-1|1}}\cdot\frac{\mathfrak{B}_{2n-1}}{2n}.$$

Diese Formeln hat schon *Moivre* auf anderem Wege gefunden.

§. 4.

Um eine zweite Bildungsweise zu erhalten, setze man allgemein

$$7. \quad S(x,n)=B(n,n+1).x^{n+1}+B(n,n).x^n+B(n,n-1).x^{n-1}+B(n,n-2).x^{n-2}+\dots$$

$$\dots+B(n,n-m+1).x^{n-m+1}+\dots+B(n,2).x^2+B(n,1).x^1.$$

Hier ist zu bemerken, dafs alle Coëfficienten von der Form $B(n,n-2)$, $B(n,n-4)$, ... $B(n,n-2p-2)=0$ sind, und dafs die Bildungsweise der beiden ersten Glieder von derjenigen der folgenden Glieder verschieden ist. Man hat nämlich nach Gl. 3. und 4.

$$8. \quad \begin{cases} B(n,n+1)=\dfrac{1}{n+1}, \\ B(n,n)=\dfrac{1}{2}, \\ B(n,n-2m-1)=(-)^m.\dfrac{n^{2m+1|-1}}{1^{2m+1|1}}\cdot\dfrac{\mathfrak{B}_{2m+1}}{2m+2}. \end{cases}$$

Ferner ergiebt sich noch, dafs die Werthe dieser spätern Coëfficienten allein durch die Werthe von n und m bestimmt werden.

Durch die Verbindung der beiden in Gl. 2. und Gl. 7. für $S(x,n)$ angegebenen Formeln läfst sich eine andere Bildungsweise der Bernoullischen Zahlen entwickeln. Da nämlich nach Gl. 2.

$$S(x,n) = x.S(x,n-1) - \underset{y=1,2,\ldots(x-1)}{\Sigma y}.S(y,n-1)$$

und nach Gl. 7.

$$S(y,n-1) = \underset{m=0,1,2,\ldots(n-1)}{\Sigma_m}.B(n-1),n-m).y^{n-m}$$

gesetzt werden kann, so hat man nur für $S(y,n-1)$ diese Reihe in den obigen Ausdruck für $S(x,n)$ einzuführen.

Es ist aber

$$S(x,n) = x.S(x,n-1) - \underset{y=1,2,\ldots(x-1)}{\Sigma y}.S(y,n-1$$

$$= (x+1)S(x,n-1) - \underset{y=1,2,\ldots x.}{\Sigma y}.S(y,n-1)$$

Ferner ist nach Gl. 7.

$$S(1,n-1) = B(n-1,n).1^n + B(n-1,n-1).1^{n-1} + \ldots + B(n-1,n-m).1^{n-m} + \ldots + B(n-1,1).1^1,$$

$$S(2,n-1) = B(n-1,n).2^n + B(n-1,n-1).2^{n-1} + \ldots + B(n-1,n-m).2^{n-m} + \ldots + B(n-1,1).2^1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$S(y,n-1) = B(n-1,n).y^n + B(n-1,n-1).y^{n-1} + \ldots + B(n-1,n-m).y^{n-m} + \ldots + B(n-1,1).y^1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$S(x,n-1) = B(n-1,n).x^n + B(n-1,n-1).x^{n-1} + \ldots + B(n-1,n-m).x^{n-m} + \ldots + B(n-1,1).x^1.$$

Zählt man diese Reihen zusammen, so ergiebt sich, da

$$1^{n-m} + 2^{n-m} + \ldots + x^{n-m} = S(x,n-m) \text{ ist,}$$

$$\underset{y=1,2,\ldots x}{\Sigma y}.S(y,n-1) = B(n-1,n).S(x,n) + B(n-1,n-1).S(x,n-1) + \ldots$$
$$\ldots + B(n-1,n-m).S(x,n-m) + \ldots + B(n-1,1).S(x,1).$$

Daher wird

$$S(x,n) = (x+1).S(x,n-1) - B(n-1,n).S(x,n) - B(n-1,n-1).S(x,n-1) - \ldots$$
$$\ldots - B(n-1,n-m).S(x,n-m) - \ldots - B(n-1,1).S(x,1),$$

oder

$$(1+B(n-1,n)).S(x,n) = (x+1).S(x,n-1) - B(n-1,n-1).S(x,n-1) - \ldots$$
$$\ldots - B(n-1,n-m).S(x,n-m) - \ldots - B(n-1,1).S(x,1).$$

Führt man in diesen Ausdruck die Werthe von $S(x,n-1)$, bis $S(x,1)$ aus der Gl. 7. ein und ordnet die Reihen nach den Potenzen von x, so erhält man

$$(1+B(n-1,n)).S(x,n)$$

$$= B(n-1,n).x^{n+1} + x^n.[B(n-1,n-1) + B(n-1,n) - B(n-1,n).B(n-1,n-1)],$$

$$+ x^{n-1}.[B(n-1,n-2) + B(n-1,n-1) - B(n-1,n-1).B(n-1,n-1) - B(n-1,n-2).B(n-2,n-1)]$$

$$+ \ldots\ldots\ldots\ldots\ldots\ldots$$

$$+ x^{n-m+1}.\left\{\begin{array}{l} + B(n-1,n-m) + B(n-1,n-m+1) - B(n-1,n-1).B(n-1,n-m+1)) \\ - B(n-1,n-2).B(n-2,n-m+1) - \ldots - B(n-1,n-p).B(n-p,n-m+1) - \ldots \\ \ldots - B(n-1,n-m).B(n-m,n-m+1) \end{array}\right\}$$

$$+ \ldots\ldots\ldots\ldots\ldots\ldots$$

$$+ x^1.[B(n-1,1) - B(n-1,n-1).B(n-1,1) - B(n-1,n-2).B(n-2,1) - \ldots - B(n-1,1).B(1,1)].$$

Diese Reihe ist mit der in Gl. 7. angegebenen identisch, und somit müssen die Coëfficienten gleich hoher Potenzen von x ebenfalls identisch sein. Dadurch erhält man folgende allgemeine zurücklaufende Bildungsweise dieser Coëfficienten:

$$9. \quad B(n,n-m+1) = \frac{1}{1+B(n-1,n)}\Big[B(n-1,n-m)+B(n-1,n-m+1) \\ - B(n-1,n-1).B(n-1,n-m+1) \\ - B(n-1,n-2).B(n-2,n-m+1) \\ - \ldots\ldots\ldots\ldots \\ - B(n-1,n-p).B(n-p,n-m+1) \\ - \ldots\ldots\ldots\ldots \\ - B(n-1,n-m).B(n-m,n-m+1)\Big].$$

Führt man nun die Zahlwerthe der drei ersten Coëfficienten, nämlich

$$B(n,n+1) = \frac{1}{n+1}, \quad B(n,n+1) = \frac{1}{2}, \quad B(n,n-1) = \frac{n}{12}$$

in die Gl. 9. ein, setzt daselbst $2m+2$ statt m und berücksichtigt, dafs

$$B(n-1,n-2m-2) - B(n-1,n-2m-2).B(n-2m-2,n-2m-1) \\ = \frac{n-2m-2}{n-2m-1}.B(n-1,n-2m-2)$$

und

$$B(n-1,n-2m-1) - B(n-1,n-1).B(n-1,n-2m-1) \\ - B(n-1,n-2m-1).B(n-2m-1,n-2m-1) = 0$$

ist, und dafs alle Coëfficienten von der Form $B(n-1,n-2p-1) = 0$ sind, so erhält man für die spätern Coëfficienten der Reihe $S(x,n)$ folgende Bildungsweise:

$$10. \quad B(n,n-2m-1) = \\ \frac{n}{n+1}.\Big[\frac{n-2m-2}{n-2m-1}.B(n-1,n-2m-2) - B(n-1,n-2).B(n-2,n-2m-1) \\ - B(n-1,n-4).B(n-4,n-2m-1) - \ldots\ldots \\ - B(n-1,n-2p).B(n-2p,n-2m-1) - \ldots\ldots \\ - B(n-1,n-2m).B(n-2m,n-2m-1)\Big].$$

Nach dieser Formel können nur die spätern, nicht aber die drei ersten Coëfficienten der Reihe für $S(x,n)$ berechnet werden.

Setzt man nach Gl. 8.

$$B(n,n-2m-1) = (-)^m.\frac{n^{2m+1|-1}}{1^{2m+1|-1}}.\frac{\mathfrak{B}_{2m+1}}{2m+2},$$

also

$$B(n+1,n-2p) \times B(n-2p,n-2m-1) = \\ (-)^{m-1}.\frac{(n-1)^{2m|-1}}{1^{2m|1}}.\frac{(2m)^{2p-1|-1}}{1^{2p-1|1}}.\frac{\mathfrak{B}_{2p-1}}{2p} \times \frac{\mathfrak{B}_{2m-2p+1}}{2m-2p+2},$$

so wird

$$B(n,n-2m-1) = \frac{n}{n+1}\cdot\frac{n-2m-2}{n-2m-1}\cdot B(n-1,n-2m-2)$$
$$+(-)^m\cdot\frac{n}{n+1}\cdot\frac{(n-1)^{2m|-1}}{1^{2m|1}}\cdot\Sigma p\,\frac{(2m)^{2p-1|-1}}{1^{2p-1|1}}\cdot\frac{\mathfrak{B}_{2p-1}}{2p}\cdot\frac{\mathfrak{B}_{2m-2p+1}}{2m-2p+2}.$$

Um die Gröfse $B(n-1,n-2m-2)$ zu entfernen, setze man zur Abkürzung die von n unabhängige, durch Σp bezeichnete Reihe $=z$, so erhält man:

$$B(n,n-2m-1)=\frac{n}{n+1}\cdot\frac{n-2m-2}{n-2m-1}\cdot B(n-1,n-2m-2)+\frac{n}{n+1}\cdot\frac{(n-1)^{2m|-1}}{1^{2m-1}}\cdot z,$$
$$B(n-1,n-2m-2)=\frac{n-1}{n}\cdot\frac{n-2m-3}{n-2m-2}\cdot B(n-2,n-2m-3)+\frac{n-1}{n}\cdot\frac{(n-2)^{2m|-1}}{1^{2m|1}}\cdot z,$$
$$B(n-2,n-2m-3)=\frac{n-2}{n-1}\cdot\frac{n-2m-4}{n-2m-3}\cdot B(n-3,n-2m-4)+\frac{n-2}{n-1}\cdot\frac{(n-3)^{2m|-1}}{1^{2m|1}}\cdot z,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$B(n-s+1,n-2m-s) = \frac{n-s+1}{n-s+2}\cdot\frac{n-2m-s-1}{n-2m-s}\cdot B(n-s,n-2m-s-1)$$
$$+\frac{n-s+1}{n-s+2}\cdot\frac{(n-s)^{2m|-1}}{1^{2m|-1}}\cdot z.$$

Da aber für $s=n-2m-1$, $B(2m+1,0)=0$ wird, so hat man

$$B(n,n-2m-1)$$
$$=\frac{z}{(n+1)(n-2m-1)}\cdot\frac{1}{1^{2m|1}}\cdot[(n-2m-1)^{2m+2|1}+(n-2m-2)^{2m+2|1}+\ldots+1^{2m+2|1}]$$
$$=z\cdot\frac{2m+1}{2m+3}\cdot\frac{n^{2m+1|-1}}{1^{2m+1|1}},$$

oder, wenn für z und $B(n,n-2m-1)$ die obigen Werthe eingeführt werden:

$$11.\quad \frac{\mathfrak{B}_{2m+1}}{2m+2}=\frac{2m+1}{2m+3}\cdot\Big[\frac{(2m)^{1|-1}}{1^{1|-1}}\cdot\frac{\mathfrak{B}_1}{2}\cdot\frac{\mathfrak{B}_{2m-1}}{2m}$$
$$+\frac{(2m)^{3|-1}}{1^{3|1}}\cdot\frac{\mathfrak{B}^3}{4}\cdot\frac{\mathfrak{B}_{2m-3}}{2m-2}$$
$$+\ldots\ldots\ldots$$
$$+\frac{(2m)^{2p-1|-1}}{1^{2p-1|1}}\cdot\frac{\mathfrak{B}_{2p-1}}{2p}\cdot\frac{\mathfrak{B}_{2m-2p+1}}{2m-2p+2}$$
$$+\ldots\ldots\ldots$$
$$+\frac{(2m)^{2m-3|-1}}{1^{2m-3|1}}\cdot\frac{\mathfrak{B}_{2m-3}}{2m+2}\cdot\frac{\mathfrak{B}_3}{4}$$
$$+\frac{(2m)^{2m-1|-1}}{1^{2m-1|1}}\cdot\frac{\mathfrak{B}_{2m-1}}{2m-1}\cdot\frac{\mathfrak{B}_1}{2}\Big];$$

oder auch, da

$$(2m+2)\cdot\frac{2m+1}{2m+3}\cdot\frac{(2m)^{2p-1|-1}}{1^{2p-1|1}}\cdot\frac{1}{2p}\cdot\frac{1}{2m-2p+2}=\frac{1}{2m+3}\cdot\frac{(2m+2)^{2p|-1}}{1^{2p|1}}$$

ist,

$$12.\quad (2m+3).\mathfrak{B}_{2m+1} = \frac{(2m+2)^{2|-1}}{1^{2|1}}.\mathfrak{B}_1 \times \mathfrak{B}_{2m-1}$$
$$+ \frac{(2m+2)^{4|-1}}{1^{4|1}}.\mathfrak{B}_3 \times \mathfrak{B}_{2m-3}$$
$$+ \dots\dots\dots\dots$$
$$+ \frac{(2m+2)^{2p|-1}}{1^{2p|1}}.\mathfrak{B}_{2p-1} \times \mathfrak{B}_{2m-2p+1}$$
$$+ \dots\dots\dots\dots$$
$$+ \frac{(2m+2)^{2m-2|-1}}{1^{2m-2|1}}.\mathfrak{B}_{2m-3} \times \mathfrak{B}_3$$
$$+ \frac{(2m+2)^{2m|-1}}{1^{2m|1}}.\mathfrak{B}_{2m-1} \times \mathfrak{B}_1.$$

Dieser Ausdruck giebt gleichfalls das Gesetz der zurücklaufenden Bildungsweise für $\mathfrak{B}_{2m+1}$ an, und wurde schon früher von *L. Euler* in seinem Instit. Calcul. diff. II. §. 123. mitgetheilt.

III. Aufsuchung der unabhängigen Bildungsweise der Bernoullischen Zahlen.

§. 5.

Die Gleichungen 5., 6. und die Gleichungen 11., 12. geben die zurücklaufende Bildungsweise und können auf verschiedenen Wegen zur unabhängigen führen, von welchen Wegen ich die interessantesten, die ich aufgefunden habe, hier mittheile.

Je nachdem man die Gl. 5. oder die Gl. 6. anwendet, erhält man zwei verschiedene Bildungsformen. Bei beiden tritt das Gesetz deutlich hervor, nach welchem die Bernoullischen Zahlen entstehen; aber auch bei der Anwendung der Gl. 11. zeigt sich ein eigenthümliches, von den andern verschiedenes Gesetz, welches jedoch die Natur dieser Zahlen weniger deutlich erkennen läfst.

Setzt man in der Gl. 5. zur Abkürzung

$$\frac{\mathfrak{B}_{2p+1}}{2p+2} = B_{2p+1},$$

so geht dieselbe in folgende über:

$$(-)^n.2n.B_{2n-1} =$$
$$-\frac{2n-1}{2(2n+1)} + \frac{(2n)^{1|-1}}{1^{1|1}}.B_1 - \frac{(2n)^{3|-1}}{1^{3|1}}.B_3 + - \dots (-)^p.\frac{(2n)^{2p+1|-1}}{1^{2p+1|1}}.B_{2p+1} + - \dots$$
$$\dots (-)^{n-3}.\frac{(2n)^{2n-5|-1}}{1^{2n-5|1}}.B_{2n-5} + (-)^{n-2}.\frac{(2n)^{2n-3|-1}}{1^{2n-3|1}}.B_{2n-3}.$$

Führt man hier den Werth von B_{2n-3} ein, so ergiebt sich

$$(-)^n.2n.B_{2n-1} = -\frac{2n-1}{2(2n+1)} + \frac{(2n)^{2|-1}}{1^{3|1}}.\frac{2n-3}{2(2n-1)}$$
$$+\left(\frac{(2n)^{1|-1}}{1^{1|1}} - \frac{(2n)^{1|-1}}{1^{1|1}}.\frac{(2n-1)^{2|-1}}{1^{3|1}}\right).B_1$$
$$-\left(\frac{(2n)^{3|-1}}{1^{3|1}} - \frac{(2n)^{3|-1}}{1^{3|1}}.\frac{(2n-3)^{2|-1}}{1^{3|1}}\right).B_3$$
$$\pm \cdots\cdots\cdots\cdots$$
$$(-)^p.\left(\frac{(2n)^{2p+1|-1}}{1^{2p+1|1}} - \frac{(2n)^{2p+1|-1}}{1^{2p+1|1}}.\frac{(2n-2p-1)^{2|-1}}{1^{3|1}}\right).B_{2p+1}$$
$$-+ \cdots\cdots\cdots\cdots$$
$$(-)^{n-4}.\left(\frac{(2n)^{2n-7|-1}}{1^{2n-7|1}} - \frac{(2n)^{2n-7|-1}}{1^{2n-7|1}}.\frac{7^{2|-1}}{1^{3|1}}\right).B_{2n-7}$$
$$(-)^{n-3}.\left(\frac{(2n)^{2n-5|-1}}{1^{2n-5|1}} - \frac{(2n)^{2n-5|-1}}{1^{2n-5|1}}.\frac{5^{2|-1}}{1^{3|1}}\right).B_{2n-5}.$$

Führt man ebenso in diesen Ausdruck den Werth von B_{2n-5} ein, so erhält man

$$(-)^n.2n.B_{2n-1} =$$
$$-\frac{2n-1}{2(2n+1)} + \frac{(2n)^{2|-1}}{1^{3|1}}.\frac{2n-3}{2(2n-1)} + \frac{(2n)^{4|-1}}{1^{5|1}}.\left(1-\frac{5^{2|-1}}{1^{3|1}}\right).\frac{2n-5}{2(2n-3)}$$
$$+\left(\frac{(2n)^{1|-1}}{1^{1|1}} - \frac{(2n)^{2|-1}}{1^{3|1}}.\frac{(2n-2)^{1|-1}}{1^{1|1}} - \frac{(2n)^{4|-1}}{1^{5|1}}\left(1-\frac{5^{2|-1}}{1^{3|1}}\right).\frac{(2n-4)^{1|-1}}{1^{1|1}}\right).B_1$$
$$-+ \cdots\cdots\cdots\cdots$$
$$(-)^p.\left(\frac{(2n)^{2p+1|-1}}{1^{2p+1|1}} - \frac{(2n)^{2|-1}}{1^{3|1}}.\frac{(2n-2)^{2p+1|-1}}{1^{2p+1|1}} - \frac{(2n)^{4|-1}}{1^{5|1}}.\left(1-\frac{5^{2|-1}}{1^{3|1}}\right).\frac{(2n-4)^{2p+1|-1}}{1^{2p+1|-1}}\right).B_{2p+1}$$
$$-+ \cdots\cdots\cdots\cdots$$
$$(-)^{n-4}.\left(\frac{(2n)^{2n-7|-1}}{1^{2n-7|1}} - \frac{(2n)^{2|-1}}{1^{3|1}}.\frac{(2n-2)^{2n-7|-1}}{1^{2n-7|1}} - \frac{(2n)^{4|-1}}{1^{5|1}}.\left(1-\frac{5^{2|-1}}{1^{3|1}}\right).\frac{(2n-4)^{2n-7|-1}}{1^{2n-7|1}}\right).B_{2n-7}.$$

Die drei ersten Glieder dieser Reihe sind von B unabhängig, und durch jede weitere Einführung eines B tritt ein neues Glied hinzu. So erhält man z. B. durch weitere Einführung von B_{2n-7} das vierte Glied mit

$$\frac{(2n)^{6|-1}}{1^{7|1}}.\left(1-\frac{7^{2|-1}}{1^{3|1}} - \frac{7^{4|-1}}{1^{5|1}}.\left(1-\frac{5^{2|-1}}{1^{3|1}}\right)\right).\frac{2n-7}{2.(2n-5)};$$

ferner durch Einführung von B_{2n-9} das fünfte Glied mit

$$\frac{(2n)^{8|-1}}{1^{9|1}}\left[1-\frac{9^{2|-1}}{1^{3|1}} - \frac{9^{4|-1}}{1^{5|1}}\left(1-\frac{5^{2|-1}}{1^{3|1}}\right) - \frac{9^{6|-1}}{1^{7|1}}.\left(1-\frac{7^{2|-1}}{1^{3|1}} - \frac{7^{4|-1}}{1^{5|1}}\left(1-\frac{5^{2|-1}}{1^{3|1}}\right)\right)\right]\times\frac{2n-9}{2.(2n-7)}.$$

Hieraus läfst sich ein Gesetz schon deutlich erkennen. Setzt man nemlich

$$\mathfrak{b}_5 = 1-\frac{5^{2|-1}}{1^{3|1}},$$
$$\mathfrak{b}_7 = 1-\frac{7^{2|-1}}{1^{3|1}} - \frac{7^{4|-1}}{1^{5|1}}.\left(1-\frac{5^{2|-1}}{1^{3|1}}\right)$$
$$= 1-\frac{7^{2|-1}}{1^{3|1}} - \frac{7^{4|-1}}{1^{5|1}}.\mathfrak{b}_5,$$

$$\mathfrak{b}_9 = 1 - \frac{9^{2|-1}}{1^{3|1}} - \frac{9^{4|-1}}{1^{5|1}}.\left(1 - \frac{5^{2|-1}}{1^{3|1}}\right) - \frac{9^{6|-1}}{1^{7|1}}.\left(1 - \frac{7^{2|-1}}{1^{3|1}} - \frac{7^{4|-1}}{1^{5|1}}\left(1 - \frac{5^{2|-1}}{1^{3|1}}\right)\right)$$

$$= 1 - \frac{9^{2|-1}}{1^{3|1}} - \frac{9^{4|-1}}{1^{5|1}}.\mathfrak{b}_5 - \frac{9^{6|-1}}{1^{7|1}}.\mathfrak{b}_7,$$

$$\mathfrak{b}_{11} = 1 - \frac{11^{2|-1}}{1^{3|1}} - \frac{11^{4|-1}}{1^{5|1}}.\mathfrak{b}_5 - \frac{11^{6|-1}}{1^{7|1}}.\mathfrak{b}_7 - \frac{11^{8|-1}}{1^{9|1}}.\mathfrak{b}_9,$$

u. s. w.,

so erhält man allgemein, wenn wieder $\mathfrak{B}_{2n-1}$ statt $2n.B_{2n-1}$ gesetzt wird,

$$13.\quad (-)^n.\mathfrak{B}_{2n-1} = -\frac{2n-1}{2.(2n+1)} + \frac{(2n)^{2|-1}}{1^{3|1}}.\frac{2n-3}{2.(2n+1)} + \frac{(2n)^{4|-1}}{1^{5|1}}.\frac{2n-5}{2.(2n-3)}.\mathfrak{b}_5$$

$$+ \frac{(2n)^{6|-1}}{1^{7|1}}.\frac{2n-7}{2.(2n-5)}.\mathfrak{b}_7 + \dots + \frac{(2n)^{2p|-1}}{1^{2p+1|1}}.\frac{2n-2p-1}{2.(2n-2p+1)}\mathfrak{b}_{2p+1} + \dots$$

$$\dots\dots + \frac{(2n)^{2n-4|-1}}{1^{n-3|1}}.\frac{3}{2.5}.\mathfrak{b}_{2n-3} + \frac{(2n)^{2n-2|-1}}{1^{2n-1|1}}.\frac{1}{2.3}.\mathfrak{b}_{2n-1} \quad \text{und}$$

$$14.\quad \mathfrak{b}_{2p+1} = 1 - \frac{(2p+1)^{2|-1}}{1^{3|1}} - \frac{(2p+1)^{4|-1}}{1^{5|1}}.\mathfrak{b}_5 - \frac{(2p+1)^{6|-1}}{1^{7|1}}.\mathfrak{b}_7 - \dots - \frac{(2p+1)^{2p-2|-1}}{1^{2p-2|1}}.\mathfrak{b}_{p-1}.$$

Die Gröfse $\mathfrak{b}_{2p+1}$ bedeutet Verbindungen von eigenthümlicher Art. Es entsteht nämlich eine Anzahl von 2^{p-1} Verbindungen zu 0, 1, 2, ..., $(p-1)$ Elementen, welche aus der Gröfse $1 = \frac{(2p+1)^{0|-1}}{1^{1|1}}$ und den übrigen $\frac{1}{2}p(p-1)$ Elementen von der Form $\frac{(2p+1)^{2q|-1}}{1^{2q+1|1}}$, worin dem q alle Werthe von 1 bis $p-1$ und dem p alle Werthe von 2 bis p gegeben werden müssen, zusammengesetzt sind. Diese Verbindungen sind positiv oder negativ, je nachdem eine gerade oder eine ungerade Anzahl von Elementen darin enthalten ist. Bezeichnet man nun durch $\mathfrak{b}(2p+1, q)$ sämmtliche Verbindungen zu q Elementen, so wird

$$15.\quad \mathfrak{b}_{2p+1} = 1 - \mathfrak{b}(2p+1,1) + \mathfrak{b}(2p+1,2) - + \dots (-)^q.\mathfrak{b}(2p+1,q) + \dots$$

$$\dots (-)^{p-1}.\mathfrak{b}(2p+1, p-1).$$

Man erhält die Verbindung zu 1 Element, wenn man aus den Gröfsen $\mathfrak{b}_5$, $\mathfrak{b}_7$, ..., $\mathfrak{b}_{2p-1}$ die Zahl 1, die Verbindungen zu q Elementen aber, wenn man aus den Gröfsen $\mathfrak{b}_{2q+1}$, $\mathfrak{b}_{2q+2}$, ..., $\mathfrak{b}_{2p-1}$ die Verbindungen zu $q-1$ Elementen in die Gl. 15. einführt. Hieraus ergiebt sich leicht folgende Bildungsweise dieser Verbindungen:

$$16.\quad \mathfrak{b}(2p+1, q)$$

$$= \frac{(2p+1)^{2q|-1}}{1^{2q+1|1}}.\mathfrak{b}(2q+1, q-1) + \frac{(2p+1)^{2q+2|-1}}{1^{2q+3|1}}.\mathfrak{b}(2q+3, q-1) + \dots$$

$$+ \frac{(2p+1)^{2q+2s|-1}}{1^{2q+2s+1|1}}.\mathfrak{b}(2q+2s+1, q-1) + \dots + \frac{(2p+1)^{2p-2|-1}}{1^{2p-1|1}}.\mathfrak{b}(2p-1, q-1);$$

wobei zu bemerken ist, dafs $\mathfrak{b}(2p+1,0) = 1$ gesetzt werden mufs.

Diese Gleichung giebt nicht allein die Art an, wie die Verbindungen gebildet werden müssen, sondern sie enthält auch den Weg zur unmittelbaren Berechnung derselben.

Da nämlich $\mathfrak{b}(2p+1,0)=1$ ist, so wird

$$\mathfrak{b}(2p+1,1)=\frac{(2p+1)^{2|-1}}{1^{3|1}}+\frac{(2p+1)^{4|-1}}{1^{5|1}}+\ldots+\frac{(2p+1)^{2q|-1}}{1^{2q+1|1}}+\ldots+\frac{(2p+1)^{2p-2|-1}}{1^{2p-1|1}}$$
$$=\frac{1}{2p+2}\cdot\left[-\frac{(2p+2)^{1|-1}}{1^{1|1}}-\frac{(2p+2)^{2p+1|-1}}{1^{2p+1|1}}+\frac{2^{2p+2}}{2}\right]$$
$$=-2+\frac{2^{2p+1}}{2p+2}.$$

Führt man nun in die Gleichung

$$\mathfrak{b}(2p+1,2)=$$
$$\frac{(2p+1)^{4|-1}}{1^{5|1}}.\mathfrak{b}(5,1)+\frac{(2p+1)^{6|-1}}{1^{7|1}}.\mathfrak{b}(7,1)+\ldots+\frac{(2p+1)^{2p-2|-1}}{1^{2p-1|1}}.\mathfrak{b}(2p-1,1)$$

die Werthe von $\mathfrak{b}(5,1)$, $\mathfrak{b}(7,1)$, ... $\mathfrak{b}(2p-1,1)$ ein, so erhält man

$$\mathfrak{b}(2p+1,2)=-2.\left[\frac{(2p+1)^{4|-1}}{1^{5|1}}+\frac{(2p+1)^{6|-1}}{1^{7|1}}+\ldots+\frac{(2p+1)^{2p-2|-1}}{1^{2p-1|1}}\right]$$
$$+\frac{(2p+1)^{4|-1}}{1^{5|1}}.\frac{2^{5}}{6}+\frac{(2p+1)^{6|-1}}{1^{7|1}}.\frac{2^{7}}{8}+\ldots+\frac{(2p+1)^{2p-2|-1}}{1^{2p-1|1}}.\frac{2^{2p-1}}{2p},$$

also

$$\mathfrak{b}(2p+1,2)=3-3.\frac{2^{2p+2}}{2.(2p+2)}+\frac{1}{2^{2}.(2p+2)^{2|1}}.(3^{2p+3}-3).$$

Auf diesem Wege findet sich allgemein:

$$17.\quad (-)^{q}.\mathfrak{b}(2p+1,q)$$
$$=\frac{(q+1)^{1|-1}}{1^{1|1}}-\frac{(q+1)^{2|-1}}{1^{2|1}}.\frac{1}{2.(2p+2)}.r_2+\frac{(q+1)^{3|-1}}{1^{3|1}}.\frac{1}{2^{2}.(2p+2)^{2|1}}.r_3$$
$$-+-\ldots(-)^{s-1}.\frac{(q+1)^{s|-1}}{1^{s|1}}.\frac{1}{2^{s-1}.(2p+2)^{s-1|-1}}.r_s+-\ldots$$
$$(-)^{q}.\frac{(q+1)^{q+1|-1}}{1^{q+1|1}}.\frac{1}{2^{q}.(2p+2)^{q|-1}}.r_{q+1},$$

wo

$$18.\quad r_s=s^{2p+s}-\frac{s^{1|-1}}{1^{1|1}}.(s-2)^{2p+s}+\frac{s^{2|-1}}{1^{2|1}}.(s-4)^{2p+s}-\frac{s^{3|-1}}{1^{3|1}}.(s-6)^{2p+s}+-\ldots$$

ist. Die Reihe bricht ab, sobald ein Glied $=0$ oder negativ wird.

Werden hiernach die Werthe von $\mathfrak{b}(2p+1,1)$, $\mathfrak{b}(2p+1,2)$, ..., $\mathfrak{b}(2p+1,p-1)$ berechnet und in Gl. 15. eingeführt, so erhält man durch Ordnen des Ganzen nach r folgende Bildungsweise für $\mathfrak{b}_{2p+1}$:

$$19.\quad \mathfrak{b}_{2p+1} = \frac{(p+1)^{2|-1}}{1^{2|1}} - \frac{(p+1)^{3|-1}}{1^{3|1}} \cdot \frac{1}{2.(2p+2)} \cdot r_2 + \frac{(p+1)^{4|-1}}{1^{4|1}} \cdot \frac{1}{2^2.(2p+2)^{2|1}} \cdot r_3$$
$$- \frac{(p+1)^{5|-1}}{1^{5|1}} \cdot \frac{1}{2^3.(2p+2)^{3|1}} \cdot r_4 + - \ldots (-)^{p-1} \cdot \frac{(p+1)^{p+1|-1}}{1^{p+1|1}} \cdot \frac{1}{2^{p-1}.(2p+2)^{p-1|-1}} \cdot r_p,$$

wo ebenfalls, wie in Gl. 18.,

$$r_2 = 2^{2p+2},$$
$$r_3 = 3^{2p+3} - \frac{3^{1|-1}}{1^{1|1}},$$
$$r_4 = 4^{2p+4} - \frac{4^{1|-1}}{1^{1|1}} \cdot 2^{2p+4}$$

u. s. w., gesetzt werden mufs.

Führt man nach dieser Formel die Werthe von $\mathfrak{b}_5$, $\mathfrak{b}_7$, ..., $\mathfrak{b}_{2n-1}$ in die Gl. 13. ein, und ordnet das Ganze nach r_p, so lassen sich die Coëfficienten von r ebenfalls summiren, und man erhält durch einige Umformungen folgende unabhängige Bildungsweise der $n$ten Bernoullischen Zahl:

$$20.\quad (-)^n \cdot \mathfrak{B}_{2n-1} = -\frac{n^{1|-1}}{1^{2|1}} \cdot \frac{3n-1}{1} \cdot \frac{1}{2.(2n+1)}$$
$$+ \frac{n^{2|-1}}{1^{3|1}} \cdot \frac{4n-2}{2} \cdot \frac{1}{2^2.(2n+1)^{2|1}} \cdot r_2$$
$$- \frac{n^{3|-1}}{1^{4|1}} \cdot \frac{5n-3}{3} \cdot \frac{1}{2^3.(2n+1)^{3|1}} \cdot r_3$$
$$+ \ldots\ldots\ldots\ldots$$
$$(-)^p \cdot \frac{n^{p|-1}}{1^{p+1|1}} \cdot \frac{(p+2).n-p}{p} \cdot \frac{1}{2^p.(2n+1)^{p|1}} \cdot r_p$$
$$- + \ldots\ldots\ldots\ldots$$
$$(-)^n \cdot \frac{n^{n|-1}}{1^{n+1|1}} \cdot \frac{n.(n+1)}{n} \cdot \frac{1}{2^n.(2n+1)^{n|1}} \cdot r_n,$$

wo

$$21.\quad r_p = p^{2n+p} - \frac{p^{1|-1}}{1^{1|1}} \cdot (p-2)^{2n+p} + \frac{p^{2|-1}}{1^{2|1}} \cdot (p-4)^{2n+p}$$
$$- \frac{p^{3|-1}}{1^{3|1}} \cdot (p-6)^{2n+p} + - \ldots.$$

Wenn p eine gerade Zahl ist, so ist das letzte Glied der Reihe 2^{2n+p}: ist p eine ungerade Zahl, so endigt die Reihe mit 1^{2n+p}.

§. 6.

Wird anstatt der Gl. 5. die Gl. 6. als Grundlage der Entwicklung angenommen, so erhält man, ganz auf demselben Wege, Bildungsgesetze, welche von den in Gl. 13. bis Gl. 21. angegebenen etwas verschieden sind. Es ist nämlich

$$22.\quad (-)^n.\mathfrak{B}_{2n-1}$$

$$= -\frac{2n}{(2n+1)^{2|1}} + \frac{(2n)^{1|-1}}{3^{2|1}}.\frac{n-1}{n} + \frac{(2n)^{3|-1}}{3^{4|1}}.\frac{n-2}{n-1}.\mathfrak{b}_6 + \frac{(2n)^{5|-1}}{3^{6|1}}.\frac{n-3}{n-2}.\mathfrak{b}_8 + \dots$$
$$\dots + \frac{(2n)^{p-1|-1}}{3^{2p|1}}.\frac{n-p}{n-p+1}.\mathfrak{b}_{2p+2} + \dots + \frac{(2n)^{2n-3|-1}}{3^{2n-2|1}}.\frac{1}{2}.\mathfrak{b}_{2n}$$

und

$$23.\quad \mathfrak{b}_{2p} = 1 - \frac{(2p)^{2|-1}}{3^{2|1}} - \frac{(2p)^{4|-1}}{3^{4|1}}.\mathfrak{b}_6 - \frac{(2p)^{6|-1}}{3^{6|1}}.\mathfrak{b}_8 - \dots - \frac{(2p)^{2p-4|-1}}{1^{2p-4|1}}.\mathfrak{b}_{2p-2}.$$

Die Gröfse $\mathfrak{b}_{2p}$ bedeutet eben solche Verbindungen wie $\mathfrak{b}_{2p+1}$; nur sind die Elemente, aus welchen diese Verbindungen bestehen, von jenen verschieden; daher gelten zwar auch die Gleichungen

$$24.\quad \mathfrak{b}_{2p} = 1 - \mathfrak{b}(2p,1) + \mathfrak{b}(2p,2) - + \dots (-)^q.\mathfrak{b}(2p,q) + - \dots$$
$$\dots(-)^{p-2}.\mathfrak{b}(2p,p-2)$$

und

$$25.\quad \mathfrak{b}(2p,q) = \frac{(2p)^{2q|-1}}{3^{2q|1}}.\mathfrak{b}(2q+2,q-1) + \frac{(2p)^{2q+2|-1}}{1^{2q+2|1}}.\mathfrak{b}(2q+4,q-1) + \dots$$
$$\dots + \frac{(2p)^{2p-4|-1}}{3^{2p-4|1}}.\mathfrak{b}(2p-2,q-1),$$

aber die unabhängige Bildungsweise ist folgende:

$$26.\quad (-)^q.\mathfrak{b}(2p,q)$$

$$= \frac{(q+1)^{1|-1}}{1^{1|1}} + \frac{(q+1)^{2|-1}}{1^{2|1}}.\frac{1}{(2p+1)^{2|1}}.r'_2 + \frac{(q+1)^{3|-1}}{1^{3|1}}.\frac{1}{(2p+1)^{4|1}}.r'_3 + \dots$$
$$\dots + \frac{(q+1)^{s|-1}}{1^{s|1}}.\frac{1}{(2p+1)^{2s-2|1}}.r'_s + \dots + \frac{(q+1)^{q+1|-1}}{1^{q+1|1}}.\frac{1}{(2p+1)^{2q|1}}.r'_{q+1},$$

wo

$$27.\quad r'_s = \frac{(2s)^{s-1|-1}}{1^{s-1|1}} - \frac{(2s)^{s-2|-1}}{1^{s-2|1}}.2^{2p+2s-2} + \frac{(2s)^{s-3|-1}}{1^{s-3|1}}.3^{2p+2s-2} - + \dots$$
$$\dots(-)^{s-1}.\frac{(2s)^{0|-1}}{1^{0|1}}.s^{2p+2s-2}$$

und

$$28.\quad \mathfrak{b}_{2p} = \frac{p^{2|-1}}{1^{2|1}} + \frac{p^{3|-1}}{1^{3|1}}.\frac{1}{(2p+1)^{2|1}}.r'_2 + \frac{p^{4|-1}}{1^{4|1}}.\frac{1}{(2p+1)^{4|1}}.r'_3 + \dots$$
$$+ \frac{p^{q+2|-1}}{1^{q+2|1}}.\frac{1}{(2p+1)^{2q|1}}.r'_{q+1} + \dots + \frac{p^{p|-1}}{1^{p|1}}.\frac{1}{(2p+1)^{2p-4|1}}.r'_{p-1}.$$

Durch Einführung der Werthe von $\mathfrak{b}_6$, $\mathfrak{b}_8$, ..., $\mathfrak{b}_{2n}$ in die Gl. 22. erhält man zuletzt

$$29.\quad (-)^n.\mathfrak{B}_{2n-1}$$

$$= -\frac{n^{1|-1}}{1^{1|1}}.\frac{2n}{(2n+1)^{2|1}} - \frac{n^{2|-1}}{1^{2|1}}.\frac{2n}{2.(2n+1)^{4|1}}.r'_2 - \frac{n^{3|-1}}{1^{3|1}}.\frac{2n}{3.(2n+1)^{6|1}}.r'_3 - \dots$$
$$\dots - \frac{n^{p|-1}}{1^{p|1}}.\frac{2n}{p.(2n+1)^{2p|1}}.r'_p - \dots - \frac{n^{n|-1}}{1^{n|1}}.\frac{2n}{n.(2n+1)^{2n|1}}.r'_n,$$

wo

$$30.\quad r'_p = \frac{(2p)^{p-1|-1}}{1^{p-1|1}} - \frac{(2p)^{p-2|-1}}{1^{p-2|1}}.2^{2n+2p} + \frac{(2p)^{p-3|-1}}{1^{p-3|1}}.3^{2n+2p} -+ \dots$$
$$\dots (-)^p.\frac{(2p)^{0|-1}}{1^{0|1}}.p^{2n+2p};$$

welche Gleichung eine zweite, von der in Gl. 20. verschiedene unabhängige Bildungsweise der *n*ten Bernoullischen Zahl giebt.

§. 7.

Hinsichtlich der wirklichen Berechnung der Bernoullischen Zahlen ist zu bemerken, dafs die Gl. 20. und 29. hierzu nicht wohl angewandt werden können, weil die hohen Potenzen der Zahlen die Rechnung sehr schwierig machen. So müssen z. B., wenn man $\mathfrak{B}_{13}$ nach Gl. 20. berechnen will, die Potenzen 2^{16}, 2^{18}, 2^{20}, 3^{17}, 3^{19}, 3^{21}, 4^{18}, 4^{20}, 5^{19}, 5^{21}, 6^{20}, 7^{21} eingeführt werden; nach Gl. 29. müfste man 2^{18}, 2^{20}, ..., 2^{28}, 3^{20}, 3^{22}, ..., 3^{28}, 4^{22}, 4^{24}, ... 4^{28}, 5^{24}, 5^{26}, 5^{28}, 6^{26}, 6^{28}, 7^{28} einführen. Dagegen hat die Berechnung mit Hülfe der Gl. 13. und 14. oder der Gl. 22. und 23. keine besondere Schwierigkeit. Man berechnet nämlich nach Gl. 14. oder Gl. 23. die Werthe von $\mathfrak{b}$ und führt dieselben in die Gl. 13. oder 22. ein. So erhält man z. B.

nach Gl. 14.	nach Gl. 22.
$\mathfrak{b}_5 = -\frac{7}{3}$,	$\mathfrak{b}_6 = -\frac{3}{2}$,
$\mathfrak{b}_7 = \frac{31}{3}$,	$\mathfrak{b}_8 = \frac{10}{3}$,
$\mathfrak{b}_9 = -\frac{381}{5}$,	$\mathfrak{b}_{10} = -\frac{21}{2}$,
$\mathfrak{b}_{11} = \frac{2555}{3}$,	$\mathfrak{b}_{12} = 45$,
$\mathfrak{b}_{13} = -\frac{1414477}{105}$,	$\mathfrak{b}_{14} = -\frac{7601}{30}$,
$\mathfrak{b}_{15} = 286685$,	$\mathfrak{b}_{16} = 1820$.

Führt man diese Werthe in Gl. 13. ein, so erhält man

$$\mathfrak{B}_{15} = -\frac{15}{2.17} + \frac{16^{2|-1}}{1^{3|1}}.\frac{13}{2.15} - \frac{16^{4|-1}}{1^{5|1}}.\frac{11}{2.13}.\frac{7}{3} + \frac{16^{6|-1}}{1^{7|1}}.\frac{9}{2.11}.\frac{31}{3} - \frac{16^{8|-1}}{1^{9|1}}.\frac{7}{2.9}.\frac{381}{5}$$
$$+ \frac{16^{10|-1}}{1^{11|1}}.\frac{5}{2.7}.\frac{2555}{3} - \frac{16^{12|-1}}{1^{13|1}}.\frac{3}{2.5}.\frac{1414477}{105} + \frac{16^{14|-1}}{1^{15|1}}.\frac{1}{2.3}.286685$$
$$= -\frac{15}{34} + \frac{52}{3} - \frac{1078}{3} + 4836 - \frac{127127}{3} + \frac{664300}{3} - \frac{2828954}{5} + \frac{1146740}{3}$$
$$= -\frac{15}{34} + \frac{1682887}{3} - \frac{2804774}{5} = -\frac{15}{34} + \frac{113}{15} = \frac{3617}{510}.$$

Nach Gl. 12. erhält man aber

$$\mathfrak{B}_{15} = -\frac{16}{17^{2|1}} + \frac{16^{1|-1}}{3^{2|1}}.\frac{7}{8} - \frac{16^{3|-1}}{3^{4|1}}.\frac{6}{7}.\frac{3}{2} + \frac{16^{5|-1}}{3^{6|1}}.\frac{5}{6}.\frac{10}{3} - \frac{16^{7|-1}}{3^{8|1}}.\frac{4}{5}.\frac{21}{2}$$

$$+\frac{16^{9|-1}}{3^{10|1}}.\frac{3}{4}.45 - \frac{16^{11|-1}}{3^{12|1}}.\frac{2}{3}.\frac{7601}{30} + \frac{16^{13|-1}}{3^{14|1}}.\frac{1}{2}.1820$$

$$= -\frac{8}{153} + \frac{7}{6} - 12 + \frac{650}{9} - \frac{4004}{15} + 585 - \frac{30404}{45} + \frac{910}{3}$$

$$= -\frac{8}{153} + \frac{5265}{6} - \frac{39166}{45} = -\frac{8}{153} + \frac{643}{90} = \frac{10851}{1530} = \frac{3617}{510}.$$

§. 8.

Mit Hülfe der Gl. 11. oder 12. erhält man eine von der obigen ganz verschiedene Bildungsweise. Sucht man nämlich nach dieser Gleichung die Werthe von $\mathfrak{B}_1$, $\mathfrak{B}_3$ u. s. w. auf, ohne die Berechnung wirklich auszuführen, so findet sich, dafs

$$31. \quad \frac{\mathfrak{B}_{2n+1}}{2n+2} = \frac{3}{2n+3}.1^{n|1}.2^n.\left(\frac{\mathfrak{B}_1}{2}\right)^{n+1}.R_{2n+1}$$

$$= \frac{1^{n|1}}{2n+3}.\frac{(\mathfrak{B}_1)^n}{4}.R_{2n+1}$$

gesetzt werden kann, wo R_{2n+1} eine eigenthümliche Art von Verbindungen bedeutet, deren Gesetz durch die Gleichung

$$32. \quad R_{2n+1} = \frac{(2n+1)^{0|-2}}{5^{0|2}}.R_1.R_{2n-1} + \frac{(2n+1)^{1|-2}}{5^{1|2}}.R_3.R_{2n-3} + \frac{(2n+1)^{2|-2}}{5^{2|2}}.R_5.R_{2n-5}$$

$$+\ldots + \frac{(2n+1)^{p|-2}}{5^{p|2}}.R_{2p+1}.R_{2n-2p-1} + \ldots + \frac{(2n+1)^{n-2|-2}}{5^{n-2|2}}.R_{2n-3}.R_3$$

$$+\frac{(2n+1)^{n-1|-2}}{5^{n-1|2}}.R_{2n-1}.R_1$$

ausgedrückt wird.

Da nun

$$R_1 = 1, \quad R_3 = 1$$

ist, und je zwei, gleichviel von den Enden der Reihe abstehende Glieder einander gleich sind, so kann man

$$R_{2n+1} = 2.R_{2n-1} + R(2n+1, 1),$$
$$R_{2n-1} = 2.R_{2n-3} + R(2n-1, 1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$R_9 = 2.R_7 + R(9,1),$$
$$R_7 = 2.R_5 + R(7,1),$$
$$R_5 = 2.R_3 = 2$$

setzen, und folglich ist

33. $$R_{2n+1} = 2^{n-1}+R(2n+1,\,1)+2.R(2n-1,\,1)+2^2.R(2n-3,\,1)+\cdots$$
$$\cdots+2^p.R(2n-2p+1,\,1)+\cdots+2^{n-4}.R(q,\,1)+2^{n-3}.R(7,\,1)$$
$$= 2^{n-1}+r(2n+1,\,1);$$

wo die Zeichen $R(2n+1,\,1)$ und $r(2n+1,\,1)$ nur zur Abkürzung dienen. Setzt man nun in Gl. 32.

$$R_{2p+1} = 2^{p-1}+r(2p+1,\,1),\quad R_{2n-2p+1} = 2^{n-p-2}+r(2n-2p-1,\,1),$$

so erhält man

$$R_{2n+1} = \underset{p=0,1,2,\ldots,n-1}{\Sigma_p}\cdot\frac{(2n+1)^{p|-2}}{5^{p|2}}\cdot(2^{n-3}+2^{p-1}.r(2n-2p-1,\,1)+2^{n-p-2}.r(2p+1,\,1)$$
$$+r(2p+1,\,1).r(2n-2p-1,\,1)).$$

Zählt man aber die beiden Endglieder der Reihe in Gl. 32. zusammen, setzt

$$R_{2n-1} = 2^{n-2}+r(2n-1,\,1)$$

und bemerkt, dafs $r(5,\,1) = r(3,\,1) = 0$ ist, so ergiebt sich

$$R_{2n+1} = 2^{n-1}+2^{n-3}.\left[\frac{(2n+1)^{1|-2}}{5^{1|2}}+\frac{(2n+1)^{2|-2}}{5^{2|2}}+\frac{(2n+1)^{3|-2}}{5^{3|2}}+\cdots+\frac{(2n+1)^{n-2|-2}}{5^{n-2|2}}\right]$$
$$+2.r(2n-1,\,1)+\underset{p=1,2,\ldots,n-2}{\Sigma_p}\cdot\frac{(2n+1)^{p|-2}}{5^{p|2}}\cdot(2^{p-1}.r(2n-2p-1,\,1)+2^{n-p-2}.r(2p+1,\,1)$$
$$+r(2p+1,\,1).r(2n-2p-1,\,1))$$
$$= 2^{n-1}+2^{n-3}.f(2n+1,\,n-2)+2.r(3n-1,\,1)+f'(2n+1,\,1).$$

Nach Gl. 33. ist daher

$$r(2n+1,\,1) = 2^{n-3}.f(2n+1,\,n-2)+2.r(2n-1,\,1)+f'(2n+1,\,1),$$
$$r(2n-1,\,1) = 2^{n-4}.f(2n-1,\,n-3)+2\cdot r(2n-3,\,1)+f'(2n-1,\,1),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r(11,\,1) = 2^2.f(11,\,3)+2.r(9,\,1)+f'(11,\,1),$$
$$r(\;9,\,1) = 2^1.f(9,\,2)+2.r(7,\,1),$$
$$r(\;7,\,1) = 2^0.f(7,\,1),$$

mithin

$$r(2n+1,\,1) = 2^{n-3}.[f(2n+1,\,n-2)+f(2n-1,\,n-3)+\cdots+f(9,\,2)+f(7,\,1)]$$
$$+f'(2n+1,\,1)+2.f'(2n-1,\,1)+\cdots+2^p.f'(2n-2p+1,\,1)+\cdots+2^{n-5}.f'(11,\,1)$$
$$= 2^{n-3}.c(2n+1,\,1)+r(2n+1,\,2).$$

Die durch $c(2n+1,\,1)$ bezeichnete Reihe besteht aus der Summe aller Vorzahlen, welche entstehen, wenn man in dem Ausdruck $\frac{(2n+1)^{p|-2}}{5^{p|2}}$ der Gröfse n alle ganzen Zahlenwerthe von $n = 3$ bis und einschliefslich $n = n$ und zugleich der Gröfse p alle ganzen Zahlenwerthe von $p = 1$ bis $p = n-2$ giebt; das heifst, es ist

$$34. \quad c(2n+1,1) = \frac{7^{1|-2}}{5^{1|2}} + \frac{9^{1|-2}}{5^{1|2}} + \frac{11^{1|-2}}{5^{1|2}} + \cdots + \frac{(2n+1)^{1|-2}}{5^{1|2}}$$
$$+ \frac{9^{2|-2}}{5^{2|2}} + \frac{11^{2|-2}}{5^{2|2}} + \frac{13^{2|-2}}{5^{2|2}} + \cdots + \frac{(2n+1)^{2|-2}}{5^{2|2}}$$
$$+ \frac{11^{3|-2}}{5^{3|2}} + \frac{13^{3|-2}}{5^{3|2}} + \frac{15^{3|-2}}{5^{3|2}} + \cdots + \frac{(2n+1)^{3|-2}}{5^{3|2}}$$
$$+ \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot$$
$$+ \frac{(2n-3)^{n-4|-2}}{5^{n-4|2}} + \frac{(2n-1)^{n-4|2}}{5^{n-4|2}} + \frac{(2n+1)^{n-4|-2}}{5^{n-4|2}}$$
$$+ \frac{(2n-1)^{n-3|-2}}{5^{n-3|2}} + \frac{(2n+1)^{n-3|-2}}{5^{n-3|2}}$$
$$+ \frac{(2n+1)^{n-2|-2}}{5^{n-2|2}}.$$

Daher hat man

$$R_{2n+1} = 2^{n-1} + 2^{n-3}.c(2n+1,1) + r(2n+1,2).$$

Führt man hiernach die Werthe von R_{2p+1} und $R_{2n-2p-1}$ in die Gl. 32. ein, ordnet die Producte nach den Potenzen von 2 und nach $c(2p+1,1)$ und $r(2p+1,2)$, so findet man auf demselben Wege

$$R_{2n+1} = 2^{n-1} + 2^{n-3}.c(2n+1,1) + 2^{n-5}.c(2n+1,2) + r(2n+1,3),$$

wo

$$35. \quad c(2n+1,2)$$
$$= 2.\Sigma_p.c(2p+1,1)\cdot\left[\frac{(2p+5)^{p|-2}}{5^{p|2}} + \frac{(2p+7)^{p|-2}}{5^{p|2}} + \cdots + \frac{(2n+1)^{p|-2}}{5^{p|2}}\right]$$
$$p = 3,4,\ldots,n-2$$

ist und also Verbindungen zu zwei Elementen bedeutet.

Auf diesem Wege erhält man allgemein

$$36. \quad R_{2n+1} = 2^{n-1} + 2^{n-3}.c(2n+1,1) + 2^{n-5}.c(2n+1,2) + \cdots$$
$$+ 2^{n-2p-1}.c(2n+1,p) + \cdots$$

Diese Reihe endigt entweder mit 2^1 oder 2^0, je nachdem n eine gerade oder eine ungerade Zahl ist.

Die Coëfficienten $c(2n+1,1)$, $c(2n+1,2)$, ..., $c(2n+1,p)$ bedeuten eigenthümliche Verbindungen zu 1, 2, 3, ..., p Elementen, welche nach folgendem Gesetz gebildet sind.

37. $c(2n+1,p)$

$$= 2.\Sigma_q.c(4p+2q-1,p-1)\cdot\Big[\frac{(4p+2q+3)^{2p+q-1|-2}}{5^{2p+q-1|2}}+\frac{(4p+2q+5)^{2p+q-1|-2}}{5^{2p+q-1|2}}+\cdots\cdots+\frac{(2n+1)^{2p+q-1|-2}}{5^{2p+q-1|2}}\Big]$$

$$+2.\Sigma_p.c(4p+2q-5,p-2)\cdot\Big[\frac{(4p+2q+3)^{2p+q-3|-2}}{5^{2p+q-3|2}}\cdot c(7,1)+\frac{(4p+2q+5)^{2p+q-3|-2}}{5^{2p+q-3|2}}\cdot c(9,1)+\cdots\cdots$$

$$\cdots\cdots+\frac{(2n+1)^{2p+q-3|-2}}{5^{2p+q-3|2}}\cdot c(2n-4p-2q+5,1)\Big]$$

$$+2.\Sigma_q.c(4p+2q-9,p-3)\cdot\Big[\frac{(4p+2q+3)^{2p+q-5|-2}}{5^{2p+q-5|2}}\cdot c(11,2)+\frac{(4p+2q+5)^{2p+q-5|-2}}{5^{2p+q-5|2}}\cdot c(13,2)+\cdots\cdots$$

$$\cdots\cdots+\frac{(2n+1)^{2p+q-5|-2}}{5^{2p+q-5|2}}\cdot c(2n-4p-2q+9,2)\Big]$$

. . . .

$$+2.\Sigma_q.c(4p-4r+2q+3,p-r)\cdot\Big[\frac{(4p+2q+3)^{2p-2r+q+1|-2}}{5^{2p-2r+q+1|2}}\cdot c(4r-1,r-1)+\frac{(4p+2q+5)^{2p-2r+q+1|-2}}{5^{2p-2r+q+1|2}}\cdot c(4r+1,r-1)$$

$q=0,1,2,\ldots,n-2p-1$

$$+\cdots\cdots+\frac{(2n+1)^{2p-2r+q+1|-2}}{5^{2p-2r+q+1|2}}\cdot c(2n-4p+4r-2q-3,r-1)\Big]$$

$+$ . . . .

Ist $p-r=r-1$, so kommt die Endreihe nur einmal vor; was immer alsdann eintritt, wenn p eine ungerade Zahl ist: ist p eine gerade Zahl, so mufs auch die letzte Reihe noch mit 2 multiplicirt werden.

Eine andere Bildungsweise für $c(2n+1,p)$ aufzufinden, ist mir nicht gelungen; wohl aber habe ich eine zur Berechnung zweckmäfsigere Form für $c(2n+1,1)$ gefunden, wovon ich aber hier nur die Hauptresultate angeben kann.

Man erhält durch Umformung der Reihe:

$$\Sigma_s\frac{(2p+2s+5)^{p|-2}}{5^{p|2}} = \frac{(2p+5)^{p|-2}}{5^{p|2}}+\frac{(2p+7)^{p|-2}}{5^{p|2}}+\cdots\cdots+\frac{(2n+1)^{p|-2}}{5^{p|2}}$$

$s=0,1,2,\ldots,n-p-2$

$$= \frac{2^0}{5^{0|2}}\cdot\frac{p^{0|-1}}{1^{0|1}}\cdot(n-p-1)+\frac{2^1}{5^{1|2}}\cdot\frac{p^{1|-1}}{1^{1|1}}\cdot\frac{(n-p-1)^{2|1}}{2}$$

$$+\frac{2^2}{5^{2|2}}\cdot\frac{p^{2|-1}}{1^{2|1}}\cdot\frac{(n-p-1)^{3|1}}{3}+\cdots\cdots+\frac{2^r}{5^{r|2}}\cdot\frac{p^{r|-1}}{1^{r|1}}\cdot\frac{(n-p-r)^{r+1|1}}{r+1}$$

$$+\cdots\cdots+\frac{2^p}{5^{p|2}}\cdot\frac{p^{p|-1}}{1^{p|1}}\cdot\frac{(n-2p)^{p+1|1}}{p+1}$$

und dadurch die Reihe

$$f(2n+1,n-2) = \frac{(2n+1)^{1|-2}}{5^{1|2}}+\frac{(2n+1)^{2|-2}}{5^{2|2}}+\frac{(2n+1)^{3|-2}}{5^{3|2}}+\cdots\cdots+\frac{(2n+1)^{n-2|-2}}{5^{n-2|2}}$$

$$= \frac{2^0}{5^{0|2}}\cdot\frac{(n-2)^{1|1}}{1^{1|1}}+\frac{2^1}{5^{1|2}}\cdot\frac{(n-2)^{3|1}}{2^{2|1}}+\frac{2^2}{5^{2|2}}\cdot\frac{(n-4)^{5|1}}{3^{3|1}}$$

$$+\frac{2^3}{5^{3|2}}\cdot\frac{(n-6)^{7|1}}{4^{4|1}}+\cdots\cdots+\frac{2^r}{5^{r|2}}\cdot\frac{(n-2r)^{2r+1|1}}{(r+1)^{r+1|1}}+\cdots\cdots$$

Zuletzt erhält man

$$38. \quad c(2n+1,1) = \frac{2^0}{5^{0|2}} \cdot \frac{(n-2)^{2|1}}{1^{2|1}} + \frac{2^1}{5^{1|2}} \cdot \frac{(n-2)^{4|1}}{2^{3|1}} + \frac{2^2}{5^{2|2}} \cdot \frac{(n-4)^{6|1}}{3^{4|1}}$$
$$+ \frac{2^3}{5^{3|2}} \cdot \frac{(n-6)^{8|1}}{4^{5|1}} + \dots + \frac{2^r}{5^{r|2}} \cdot \frac{(n-2r)^{2r+2|1}}{(r+1)^{r+2|1}} + \dots$$

Die Reihe endigt entweder mit $1^{n|1}$ oder mit $2^{n|1}$, je nachdem n eine ungerade oder eine gerade Zahl ist.

Berechnet man hiernach $c(2n+1,1)$, alsdann nach Gl. 37. $c(2n+1,2)$, $c(2n+1,3)$ u. s. w., und hierauf nach Gl. 36. den Werth von R_{2n+1}, so erhält man nach Gl. 31. den Werth von $\mathfrak{B}_{2n+1}$; jedoch ist dieser Weg sehr weitläufig und beschwerlich. Indessen ist es nicht uninteressant, zu sehen, dafs solche Verbindungen wie R_{2n+1}, $c(2n+1,p)$ umgeformt und in Reihen nach den Potenzen von 2 geordnet werden können.

Carlsruhe, im September 1841.

18.
Bemerkungen zu der Abhandlung No. 22. Band 26. Heft 4. dieses Journals.

(Von dem Herrn Professor *Enke* zu Berlin.)

Der Herr Professor *Reuschle* in Stuttgart hat in Heft 4. des 26ten Bandes dieses Journals einen Aufsatz „Über die Deduction der Methode der kleinsten Quadrate aus Begriffen der Wahrscheinlichkeitsrechnung" gegeben, in welchem er auch meiner Bearbeitung dieses Gegenstandes erwähnt und an zwei Stellen in derselben Anstofs nimmt. Nemlich zuerst an dem Übergange von der endlichen Summation zum Integral, und zweitens an der Zurückführung des Princips des arithmetischen Mittels auf die einfacheren Voraussetzungen, welche dabei zum Grunde liegen, oder aus denen es folgen würde.

Was den ersten Punct betrifft, den Übergang der endlichen Summation zum Integrale, so habe ich ihn allerdings nur angedeutet, weil er bei so vielen Untersuchungen vorkommt, dafs in einem speciellen Fall man annehmen kann, es sei nicht nöthig, ihn jedesmal vollständig zu deduciren. Da indessen Herr Professor *Reuschle* einen directen Zusammenhang mit der Wahrscheinlichkeitsrechnung anzunehmen scheint, so will ich hier kurz angeben, wie ich mir diesen Übergang gedacht habe. Ich möchte glauben, dafs Herr Professor *Reuschle* dieselben Schwierigkeiten in vielen andern Fällen, z. B. bei der Bestimmung der mittleren Temperatur aus einzelnen Beobachtungen finden würde, und dafs eben deshalb das hier berührte Problem im Grunde nichts mit diesen Schwierigkeiten zu thun hat.

In *Eulers* Differentialrechnung P. II. §. 121. sqq. findet sich eine Gleichung für die Summirung einer Reihe, die hier vielleicht am directesten zum Ziele führt. Wenn

$$a, \quad b, \quad c, \quad \ldots \quad v, \quad z$$

Glieder einer Reihe sind, die, wie *Euler* es ausdrückt, zum Zeiger x gehören, so dafs die einzelnen Glieder gefunden werden, wenn x gleich

$$1, \quad 2, \quad 3, \quad \ldots \quad x-1, \quad x$$

gesetzt wird, so hat man strenge:

$$\Sigma(a+b+c+\cdots+v+z) =$$
$$\int z\,dx + \tfrac{1}{2}z + \frac{B_1}{1.2}\cdot\frac{dz}{dx} - \frac{B_2}{1.2.3.4}\cdot\frac{d^3z}{dx^3} + \frac{B_3}{1.2.3.4.5.6}\cdot\frac{d^5z}{dx^5}\cdot + \text{Const.},$$

wo die Constante so bestimmt werden mufs, dafs die rechte Seite der Gleichung Null wird, wenn $x = 0$. Man erreicht dieses, wenn man dieselben Glieder, welche auf der rechten Seite für z gelten, auch für das Glied, welches dem $x = 0$ correspondirt, hinzusetzt; aber mit entgegengesetztem Zeichen.

Wenn x als Zahl eine sehr grofse Anzahl von Einheiten enthält, in Vergleich mit der Ausdehnung des ganzen Intervalls von 0 bis x, so kann man auf der rechten Seite alle Glieder aufser dem Integrale als verschwindend betrachten, weil $\frac{1}{2}z$ und das correspondirende Glied der Constante nur einzelne Glieder bei einer sehr grofsen Anzahl ähnlicher in der ganzen Summe betreffen, und die Differentiale, da sie durch die endlichen Differenzen ersetzt werden können, nothwendig ebenfalls sehr klein werden müssen, in diesem Falle. Die B_1, B_2, B_3 etc., welche die Bernoullischen Zahlen bezeichnen, bilden zwar in der Fortsetzung eine divergirende Reihe, allein es finden hier dieselben Betrachtungen Statt, wie bei ähnlichen Reihen, welche trotz dieser anscheinenden Divergenz sich einer Grenze nähern, und welche *Lagrange* „demi-convergentes" nennt.

Hiernach wird man, um so genäherter, je gröfser die Anzahl der Einheiten in der Zahl x bei sonst gleichbleibendem Intervall von 0 bis x ist, setzen können:

$$\Sigma(a+b+c\cdots+v+z) = \int_0^x z\,dx.$$

Um dieses noch augenscheinlicher zu bezeichnen, sei

$$z = \varphi(a+xw) \quad \text{und} \quad a+xw = \Delta,$$

also, wenn w und a als constant angenommen werden,

$$w\,dx = d\Delta,$$

so wird die Gleichung

$$\overset{\Delta=a+w \text{ bis } \Delta}{\Sigma}(\varphi\Delta) = \int_a^{\Delta} \varphi\Delta\cdot\frac{d\Delta}{w}$$

und überhaupt, mit der kleinen Änderung, die auch gleich bei dem ersten Übergange von der strengen Formel zur genäherten hätte eingeführt werden können, wenn a und b die Grenzwerthe von Δ sind:

$$\overset{\Delta=a \text{ bis } \Delta=b}{\Sigma}\varphi(\Delta) = \int_a^b \varphi\Delta\cdot\frac{d\Delta}{w}$$

Diese Gleichung, bei welcher vorausgesetzt wird, dafs w ein beträchtlich kleiner Theil von $b-a$ ist, bedeutet eigentlich so viel als: man kann die Summirung auf zweierlei Art ausführen, entweder indem man alle einzelnen Glieder summirt, wie auf der linken Seite angenommen wird, oder indem man die $\varphi\Delta$, welche wesentlich als unter sich gleich betrachtet werden können, jedesmal zusammennimmt und ein einzelnes $\varphi\Delta$ mit der Zahl $\frac{d\Delta}{w}$ multiplicirt, welche ausdrückt wie viele gleiche $\varphi\Delta$ einer bestimmten Gröfse vorhanden sind. Es mufs demnach die Gröfse von $d\Delta$ so gewählt werden, dafs nirgends innerhalb der Grenzen von Δ und $\Delta+d\Delta$ eine Verschiedenheit der $\varphi\Delta$ berücksichtigt zu werden braucht. Diese Vertheilung in Gruppen ist der Sinn der rechten Seite.

Wenn es möglich ist, die Gröfse von w anzugeben, oder die Gröfse des Intervalls zwischen zwei unmittelbar auf einander folgenden Δ, so kann man, da die Wahl der Einheit, in welcher man Δ ausdrückt, willkürlich ist, dieses w als Einheit nehmen, oder man kann

$$\Delta = w\Delta'$$

setzen, und folglich $a = wa'$, $b = wb'$. Es wird dann statt $\varphi\Delta$ oder $\varphi w\Delta'$ einfach $\varphi\Delta'$ geschrieben werden können, da w constant ist, und die Gleichung wird

$$\overset{\Delta'=a' \text{ bis } \Delta'=b'}{\Sigma\varphi\Delta'} = \int_{a'}^{b'} \varphi\Delta' d\Delta',$$

wo die Function $\varphi\Delta'$ auf beiden Seiten genau die nämliche ist. Dieser Fall tritt eigentlich strenge genommen bei unsern Beobachtungen wirklich ein, wenn Δ den Fehler einer einzelnen Beobachtung bedeutet, und $\varphi\Delta'$ nach meiner Definition, die ich immer noch als die directeste und bestimmteste ansehe, die Anzahl der Fehler von der Gröfse Δ, welche bei einer hinlänglich grofsen Anzahl von Beobachtungen Statt finden werden, wenn man die Anzahl der Beobachtungen gleich 1 annimmt, oder die Wahrscheinlichkeit des Fehlers Δ. Alle unsere Instrumente gehen nemlich immer bis zu einer gewissen Kleinheit der Unterabtheilungen fort; und Fehler, welche kleiner sind als die kleinsten Unterabtheilungen, die noch geschätzt werden können, kommen in den Beobachtungen selbst nicht vor. Ein Winkel-Instrument, welches durch einen Nonius bis auf 10″ getheilt ist, kann vielleicht noch 1″ zu schätzen erlauben, gewifs aber nicht 0″, 01, so dafs, wenn man mit einem solchen Instrumente einen und denselben Winkel fortwährend beobachtet, die Fehler sprungweise mindestens von 0″, 01 zu 0″, 01 fortgehend angenommen werden können. Wäre

mit einem Instrumente dieser Art gefunden worden, dafs die Anzahl der Fehler von der Gröfse x, zu der Anzahl der Fehler von der Gröfse x' sich immer durch ein bestimmtes Verhältnifs, als abhängig von der äufsersten Grenze der Fehler ... a ... und der Gröfsen x und x', wobei alle Fehler positiv genommen wären, etwa durch

$$\frac{\varphi x}{\varphi x'} = \frac{a^4 - a^2 x^2 + \frac{1}{2} x^4}{a^4 - a^2 x'^2 + \frac{1}{2} x'^4}$$

ausdrücken liefse, so kann man das Intervall 0 bis a in n Theile getheilt sich denken, von denen jeder Theil gleich der kleinsten Unterabtheilung, oder noch kleiner ist. Es wird dann die allgemeine Form von φx

$$\varphi x = C.(a^4 - a^2 x^2 + \tfrac{1}{2} x^4),$$

wo die Constante C zu bestimmen ist aus

$$\sum_0^n \varphi x = 1.$$

Für a hat man die Form nw, für x die Form mw, wenn m alle ganzen Zahlen von 0 bis n bedeutet, und die Gleichung zur Bestimmung von C wird

$$C \cdot \frac{46.n^5 + 45.n^4 - n}{60} w^4 = 1,$$

folglich, wenn man diesen Werth von C substituirt:

$$\varphi x = \frac{60 n^3}{46 n^4 + 45 n^3 - 1} \cdot \left\{1 - \frac{m^2}{n^2} + \frac{1}{2} \frac{m^4}{n^4}\right\},$$

wobei x immer die Form mw hat. Vermittels der Integration würde man aus

$$\int_0^n C \varphi m \, dm = 1$$

erhalten:

$$C = \frac{60}{46n}$$

oder

$$\varphi x = \frac{60}{46n} \cdot \left\{1 - \frac{m^2}{n^2} + \frac{1}{2} \frac{m^4}{n^4}\right\}.$$

Beide aus der endlichen Summation und aus der Integration gefundenen Werthe kommen einander um so näher, je gröfser n ist, so dafs man für die Praxis der gröfseren Bequemlichkeit wegen unbedenklich die letzte Form vorziehen kann; besonders da, wenn es auch möglich ist eine Gröfse für w anzunehmen, die Wahl dieser Gröfse doch unter einer gewissen Grenze willkürlich ist.

Nimmt man aber Δ als eine continuirliche Gröfse an, und folglich auch $d\Delta$, wie klein dieses letztere auch gegen Δ sei, so wird man die Zahl der discreten Theile in einer solchen continuirlichen Gröfse, oder den obigen Bruch

$\frac{d\varDelta}{w}$ nicht mehr durch eine Zahl ausdrücken können. Indessen unter der Voraussetzung, die in dem Begriffe einer gleichförmig stetig sich ändernden Gröfse liegt, dafs die Anzahl der discreten Theile, welche in zwei continuirlichen Gröfsen von verschiedener Ausdehnung vorkommen können, nothwendig dasselbe Verhältnifs zu einander haben müssen, wie die Ausdehnung der beiden Gröfsen zu einander, kann man diese Zurückführung auf ein bestimmtes Zahlenverhältnifs zwischen discret und continuirlich bei Seite setzen, wenn man eine andere Einheit einführt, welche dieses nicht anzugebende Zahlenverhältnifs schon einschliefst. Man ändert deshalb die Gleichung in

$$\overset{\varDelta=a \text{ bis } \varDelta=b}{\Sigma w \varphi \varDelta} = \int_a^b \varphi \varDelta \, d\varDelta$$

um und bezieht die Zahl, welche sich aus dem Integral ergiebt, auf eine neue Einheit, welche durch die Summe der $\varphi\varDelta$ definirt werden kann, die während der continuirlichen Einheit, in welcher $\varDelta$ ausgedrückt ist, Statt finden würde, wenn während dieses Intervalls $\varphi\varDelta$ constant gleich 1 wäre. Diese neue Einheit, die Flächen-Einheit bei der Quadratur, ist zwar auf der ursprünglich angenommenen bei $\varDelta$ basirt, oder auf der Längen-Einheit, aber nicht mit ihr so vergleichbar, dafs zwischen beiden ein Zahlenverhältnifs gedacht werden könnte. Hiernach addirt man in dem Integral die einzelnen Elemente, in dieser neuen Einheit ausgedrückt, zusammen, oder zieht auf der linken Seite so viele discrete Intervalle zusammen, dafs aus ihnen ein aliquoter Theil der continuirlichen Einheit entsteht, insofern angenommen wird, dafs die Anzahl der w in einem noch so kleinen $d\varDelta$ sich zu der Anzahl aller w in dem Intervall $b-a$ verhält, wie $d\varDelta$ zu $b-a$ selbst. Dafs dabei $d\varDelta$ so klein sein mufs, dafs innerhalb $\varDelta$ und $\varDelta+d\varDelta$ die Function $\varphi\varDelta$ als constant angesehen werden kann, versteht sich eben so wie oben.

Wendet man dieses Verfahren auf das vorige Beispiel an, so wird zur Bestimmung von C

$$\int_0^a C(a^4 - a^2x^2 + \tfrac{1}{5}x^4)\,dx = 1$$

oder

$$C = \frac{60}{46a^5},$$

folglich

$$\varphi x = \frac{60}{46a}\left(1 - \frac{x^2}{a^2} + \tfrac{1}{5}\frac{x^4}{a^4}\right)$$

und also die Anzahl der Fehler zwischen x und $x+dx$:

$$\varphi x\, dx = \frac{60}{46}\left(1-\frac{x^2}{a^2}+\tfrac{1}{3}\frac{x^4}{a^4}\right).\frac{dx}{a};$$

welcher Ausdruck, da $\frac{x}{a}=\frac{m}{n}$ ist, mit dem früher gefundenen φx völlig übereinstimmt, wenn

$$\frac{dx}{a}=\frac{1}{n} \quad \text{oder} \quad dx=\frac{1}{n}a,$$

das heifst, wenn dx ein so kleiner Theil von a sein könnte, dafs das Intervall dx von den zwei nächsten unmittelbar auf einander folgenden Fehlern, zwischen welchen kein anderer liegen könnte, begrenzt würde.

In den beiden Gleichungen, der hier angewandten

$$\int_0^a \varphi\Delta\, d\Delta = 1$$

und der früheren

$$\Sigma_0^a \varphi\Delta = 1,$$

bedeutet die Einheit auf der rechten Seite nicht dasselbe. In der ersteren ist es die Summe aller $\varphi\Delta$ während des Intervalls 1, wenn überall $\varphi\Delta=1$ wäre, und diese Summe wird der Anzahl der Beobachtungen gleich gesetzt. In der zweiten ist es die wirkliche Summe aller der Brüche $\varphi\Delta$, die in jedem einzelnen Puncte, wo ein Δ Statt finden kann, wirklich durch die Function $\varphi\Delta$ gegeben werden. Soll deshalb in beiden Gleichungen $\varphi\Delta$ genau Dasselbe bedeuten, so wird man in der zweiten dieselbe Hypothese machen müssen, welche bei der ersten Statt findet, das heifst, man wird in jedem der einzelnen n Puncte, in welchen ein Δ möglich ist, $\varphi\Delta=1$ setzen müssen. Die ganze Summe wird folglich $=n$, und die zweite Gleichung mufs dann heifsen:

$$\Sigma_0^a \varphi\Delta = n,$$

oder, was dasselbe ist,

$$\Sigma_0^a w\varphi\Delta = 1,$$

weil hier a selbst als Einheit angesehen, in n Theile getheilt und Δ in Theilen dieses a ausgedrückt gedacht worden ist.

Die Stelle in meiner Abhandlung, an welche Herr Prof. *Reuschle* Anstofs genommen, lautet vollständig so:

„Aufserdem liegt es in der Definition von $\varphi\Delta$, dafs für eine so grofse Anzahl von Beobachtungen, dafs alle Fehler, jeder in dem gesetzmäfsigen Verhältnifs seiner Häufigkeit, darin vorkommen,

$$m\varphi\Delta + m\varphi\Delta' + m\varphi\Delta'' \;\ldots\ldots = m,$$

oder

$$\sum_{-\infty}^{+\infty} (\varphi\varDelta) = 1 \text{ ist."}$$

„Aus dieser Form sieht man, dafs bei der unendlichen Anzahl der $\varDelta$, wenn man alle Abstufungen von $\varDelta = 0$ bis $\varDelta = a$ betrachtet, für ein bestimmtes $\varDelta$ die Function $\varphi\varDelta$ ein Unendlichkleines sein wird. Man drückt nach dem analytischen Sprachgebrauch diese Bedingung bequemer so aus, dafs man nicht die Wahrscheinlichkeit eines bestimmten Fehlers allein betrachtet, sondern die Wahrscheinlichkeit der Fehler, die innerhalb der unendlich nahen Grenzen $\varDelta$ und $\varDelta + d\varDelta$ liegen, zusammen. Innerhalb dieser unendlich nahen Grenzen wird der Werth von $\varphi\varDelta$ als constant betrachtet werden können. Hiernach ist die Wahrscheinlichkeit der Fehler zwischen $\varDelta$ und $\varDelta + d\varDelta$, $= \varphi\varDelta\, d\varDelta$, und überhaupt die Wahrscheinlichkeit der Fehler zwischen den Grenzen a und b gleich der Summe dieser Elemente innerhalb der angegebenen Grenzen, oder

$$= \int_a^b \varphi\varDelta\, d\varDelta.$$

Für die Grenzen, welche alle Fehler umfassen, $-\infty$ und $+\infty$, wird

$$\int_{-\infty}^{+\infty} \varphi\varDelta\, d\varDelta = 1,$$

gleich der Gewifsheit. Das letztere Integral giebt den Flächen-Inhalt der Wahrscheinlichkeitscurve, von der Abscissen-Axe bis zur Curve genommen. Es stellt die Anzahl von Beobachtungen vor, welche überhaupt möglich sind und alle Fehler umfassen. Jedes Flächen-Element $\varphi\varDelta d\varDelta$ giebt, damit verglichen, die Anzahl von Beobachtungen, welche, in der ganzen Anzahl, Fehler zwischen $\varDelta$ und $\varDelta + d\varDelta$ geben, oder es giebt die Anzahl von Beobachtungen mit diesen Fehlern behaftet, welche wahrscheinlich Statt finden werden, wenn die ganze Anzahl gleich 1 gesetzt wird."

So weit die Stelle aus dem astr. Jahrbuch für 1834 pag. 254 und 255. Herr Prof. *Reuschle* schiebt bei der Anführung nach dem Worte „Bedingung" die Erklärung ein: φx für ein bestimmtes x unendlich klein. Dieser Zusatz ist irrig. Die Bedingung, von welcher hier die Rede ist, ist nicht, dafs φx für ein bestimmtes x unendlich klein sein werde, weil es unendlich viele x giebt: etwas, was gar nicht Bedingung heifsen kann: sondern es ist die Gleichung $\Sigma\varphi\varDelta = 1$ selbst, in welcher eine Bedingung, der $\varphi\varDelta$ unterworfen werden mufs, liegt. So bereitwillig ich nun auch einräume, dafs in den beiden Gleichungen $\Sigma\varphi\varDelta = 1$ und $\int\varphi\varDelta d\varDelta = 1$ die Function $\varphi\varDelta$ nicht Dasselbe be-

deutet, sobald man nemlich für $d\Delta$ keine angebbare Einheit substituiren kann, in welcher Δ sich ausdrücken liefse, sondern dafs, wenn man $\varphi\Delta$ in der Bedeutung, welche es in der zweiten Gleichung hat, beibehalten will, in der ersten $\Sigma\varphi\Delta = n$ gesetzt werden müsse, oder dafs die strenge Definition von $\varphi\Delta$ jetzt so heifsen mufs: es sei die Anzahl der möglichen Stellen, in welchen ein Fehler Statt finden kann, $= n$, und eben so grofs die Anzahl der Beobachtungen; alsdann wird $\varphi\Delta$ die Anzahl der Fehler sein, welche nach der Wahrscheinlichkeitsrechnung von der Gröfse Δ vorkommen werden: so glaube ich doch, dafs wenn Herr Prof. *Reuschle* die Schwierigkeit nicht ganz wo anders gesucht hätte, als wo sie meiner Ansicht nach liegt, und wenn er, wie ich bei meinen Lesern annahm, sehr bekannte ähnliche Probleme verglichen hätte, er die angeführte Stelle nicht so bezeichnet haben würde, als sei in ihr, wie er sich ausdrückt, das Differential untergeschoben.

Bei dem zweiten Puncte der Zurückführung des Princips des arithmetischen Mittels auf einfachere Voraussetzungen hat Herr Prof. *Reuschle* mich offenbar ganz mifsverstanden. Mein Gang ist folgender. Wenn man stufenweise aufsteigt von einer geringeren Anzahl gleich guter Beobachtungen zu einer gröfseren, so findet sich zuerst, dafs wenn nur zwei Beobachtungen gegeben sind, a und b, die Annahme von $\frac{1}{2}(a+b)$, als des aus ihnen allein folgenden Resultats, auf der Hypothese beruht, dafs gleich grofse positive und negative Fehler gleiche Wahrscheinlichkeit haben. Mit dieser einzigen Hypothese reicht man aber bei einer gröfseren Zahl nicht aus; schon bei dreien nicht. Wenn nemlich a, b, c beobachtet sind, so wird man aus der Gleichheit der Beobachtungen nur schliefsen können, dafs das wahrscheinlichste Resultat eine symmetrische Function in Bezug auf a, b und c sein mufs. Um weiter zu gehen, mache ich die zweite Hypothese, dafs es möglich sein soll, das wahrscheinlichste Resultat jedesmal genau von derselben Gröfse zu finden, wenn man auch nicht die einzelnen Beobachtungen selbst kennt, sondern nur die Resultate, welche nach richtigen Principien aus beliebigen Verbindungen der einzelnen Beobachtungen unter sich abgeleitet sind. Bei drei Functionen müfste man, dieser neuen Hypothese zufolge, dieselbe symmetrische Function finden, sowohl wenn man die einzelnen a, b, c selbst kennte, als auch, wenn man blofs $\frac{1}{2}(a+b)$ und c, oder $\frac{1}{2}(a+c)$ und b, oder $\frac{1}{2}(b+c)$ und a kennte, ohne die einzelnen Werthe selbst zu benutzen. Welche Function von $\frac{1}{2}(a+b)$ und c (oder der andern beiden Verbindungen) man aber auch annimmt, so wird die Entwicklung doch nur in dem Falle eine symmetrische Function von den ein-

zelnen a, b, c geben können, wenn c eben so mit a wie mit b verbunden ist, und zwar eben so wie a mit b selbst. Die letztere Verbindung ist in $\frac{1}{2}(a+b)$ lineär. Folglich mufs c auch mit a und b eben so lineär verbunden sein, und eine Function von $a+b+c=s$ wird demnach die einzige sein, die der verlangten Bedingung Genüge thut, weil sie einmal blofs die Kenntnifs des Resultats zweier Beobachtungen, nicht die Kenntnifs der Beobachtungen selbst voraussetzt, und zweitens, weil sie in Bezug auf alle drei Gröfsen symmetrisch ist. Wählte man eine andere als diese lineäre Form $a+b+c$, so würde entweder die am Ende der Entwicklung erhaltene Function wohl in Bezug auf a und b, nicht aber in Bezug auf c symmetrisch sein können; oder es würde die Kenntnifs der einzelnen a und b, nicht blofs ihrer Summe $a+b$, dabei vorausgesetzt werden müssen. Sobald man aber dem Endresultate die Form zugesteht, dafs es nur eine Function der Summe $a+b+c$ sein darf, so giebt der Fall, dafs $a=b=c$, das arithmetische Mittel, und das Fortschreiten von 3 zu 4, 5 etc. Beobachtungen sichert dem arithmetischen Mittel die Allgemeinheit.

Den eigentlichen Nerv dieser Hypothese, die blofse Kenntnifs des Resultats früherer Beobachtungen ohne die einzelnen Data selbst zu benutzen, hat Herr Prof. *Reuschle* völlig übersehen, und sich nur an den Ausdruck „symmetrische Endfunction" gehalten. Darum sind auch alle seine angeführten Beispiele irrig, und jedes andere Beispiel wird eben so wenig treffen, wenn es nicht auf die Form einer Endfunction von $a+b+c$ zurückgeführt werden kann.

Wenn man die beiden Hypothesen annimmt, dafs erstlich die Wahrscheinlichkeit der Fehler blofs von ihrer Gröfse, nicht von ihrem Zeichen abhänge, und dafs zweitens die Herleitung des wahrscheinlichsten Resultats nicht erfordere, dafs man immer jede einzelne Beobachtung gehörig berücksichtige, sondern es auch eben so genau erhalte, wenn man die einzelnen Beobachtungen nach dem richtigen Princip gruppenweise verbindet und die Resultate der Verbindungen allein, ohne weiter die einzelnen Beobachtungen zu berücksichtigen, wieder zusammennimmt: so ist damit das arithmetische Mittel bewiesen, und die Methode der kleinsten Quadrate mit demselben. Beide Hypothesen haben die Ähnlichkeit mit einander, dafs sie die Möglichkeit der Erkenntnifs der Wahrheit bedingen: die erste in theoretischer Hinsicht, die zweite in practischer. Wenn bei den angewandten Methoden die erste Hypothese auch unrichtig ist, so können wir, insofern *nur* diese Methoden in Betracht kommen, doch nicht anders als die Hypothese machen, die Wahrheit sei nur relativ zu nehmen, in Bezug auf die Mittel, die uns zu Gebote stehen, sie zu erforschen. Die zweite

Hypothese wird durchaus nothwendig, wenn die Vermehrung der Beobachtungen uns dem Ziele näher führen soll. Denn ohne sie würde es sehr bald unausführbar für die Praxis werden, immer zu den allerersten Grundlagen zurückzugehen; ja wir nehmen sie eigentlich immer an, insofern das, was man das einfache Resultat einer Beobachtung nennt, in allen Fällen schon aus Einzelnheiten, die wir unterscheiden könnten, wenn es erforderlich wäre, zusammengesetzt ist. Der Grund weshalb ich es gleichwohl Jedem überlassen habe, ob er einfach das Princip des arithmetischen Mittels annehmen, oder bis zu diesen beiden Hypothesen zurückgehen wolle, liegt deshalb nicht darin, dafs ich an der strengen Begründung, sofern man die Hypothesen macht, irgend gezweifelt hätte, sondern weil bei Hypothesen überhaupt das Gefühl jedes Einzelnen darüber zu entscheiden hat, welche er für annehmbarer hält.

Die Veranlassung zu dieser Auseinandersetzung läfst mich noch erwähnen, dafs die gewöhnlichen Beispiele, welche bei der Wahrscheinlichkeitsrechnung zur Erläuterung gewählt werden, nemlich meistens Urnen mit verschiedenfarbigen Kugeln, oder vielseitige Prismen, die bei dem jedesmaligen Wurfe nur auf ihre Seitenflächen fallen können, für die Anwendung auf die Fehler der Beobachtungen nicht ganz zweckmäfsig zu sein scheinen. Ansprechender möchte das Folgende sein. Man denke sich eine Zielscheibe, in deren Mitte der Zielpunct angegeben ist; man lasse die verschiedenartigsten Geschosse gegen sie gerichtet sein, und bemerke die Puncte, wo diese Geschosse die Zielscheibe getroffen haben. Man stelle sich dann die Aufgabe: nach Verlöschung des eigentlichen Zielpunctes aus den vorhandenen Treffpuncten den ersteren wieder herzustellen: so werden sich an dieser Art von eigentlicher Beobachtung viele Puncte erläutern lassen. Die Erweiterung der Grenzen bis unendlich; die Verschiedenheit zwischen constanten und unregelmäfsigen Fehlern; die Verwandtschaft der Formeln für die Bestimmung des Schwerpunctes mit denen der Methode der kleinsten Quadrate; selbst die Benennung „Gewicht einer Reihe von Bestimmungen," und viele andere Erläuterungen knüpfen sich sehr anschaulich an dieses Beispiel an.

Die andern, nur kurz angedeuteten Ausstellungen des Herrn Professor *Reuschle* gegen meine Darstellungsweise, wie z. B. bei der Theorie des mittlern Fehlers pag. 357, erledigen sich von selbst durch das hier Ausgeführte.

19.

Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste.

(Von Herrn Stud. G. *Eisenstein* zu Berlin.)

Das Hauptproblem, auf welches sich alle Fragen über biquadratische Reste zurückführen lassen, erfordert für je zwei complexe Primzahlen $a+bi$ und $c+di$, erstere als ungerade vorausgesetzt, die Erforschung des Rests der Potenz $(c+di)^{\frac{1}{4}(a^2+b^2-1)}$ nach dem Modul $a+bi$, d. h. die Bestimmung derjenigen unter den vier complexen Einheiten 1, i, -1, $-i$, welcher jene Potenz nach dem Modul $a+bi$ congruent ist. Zur Lösung dieses Problems bietet sich der einfache Gedanke dar, die in Rede stehende Potenz dergestalt analytisch umzuformen, dafs in der That die Division durch den Modul allgemein ausgeführt und der Rest der Division direct beurtheilt werden könne. Dieses gelingt, wie man sehen wird, für die einfachsten Fälle, während sich die zusammengesetzteren auf jene reduciren lassen.

Von dieser Haupt-Idee geleitet, stellte ich die hier folgenden Untersuchungen an. Der gegenwärtige Beweis setzt, aufser den ersten Elementen der complexen Zahlen, durchaus nichts weiter voraus. Ich habe mich in dieser Abhandlung bemüht, alle Auseinandersetzungen so deutlich zu machen, dafs sie selbst dem Minderbewanderten zugänglich sein werden.

§. 1.

Definitionen und einfache Folgerungen.

Wenn $p_1 = a+bi$ eine ungerade complexe Primzahl (der Fall $b=0$ nicht ausgeschlossen), $p = a^2+b^2 = N(a+bi)$ ihre Norm ist, und α irgend eine nicht durch p_1 theilbare ganze complexe Zahl vorstellt, so mag der Kürze wegen das Symbol $[\alpha; p_1]$ diejenige complexe Einheit bezeichnen, welche $\equiv \alpha^{\frac{1}{4}(p-1)}$ (mod. p_1) ist. Wenn α durch p_1 theilbar ist, so soll dasselbe Symbol die *Null* bezeichnen, so dafs in allen Fällen

$$\alpha^{\frac{1}{4}(p-1)} \equiv [\alpha; p_1] \text{ (mod. } p_1) \text{ ist.}$$

Wenn während einer Untersuchung der Modul unverändert bleibt, so werde der Bequemlichkeit halber statt des Zeichens $[\alpha; p_1]$ das einfachere $[\alpha]$ mit Hinweglassung des Moduls geschrieben. Dieser Abkürzung haben wir uns, besonders im zweiten Paragraph, durchgängig bedient. Alle dort vorkommenden Symbole beziehen sich auf den Modul p_1, und es ist also kein Mifsverständnifs zu befürchten.

In Beziehung auf die eben aufgestellte Bezeichnung bemerkt man sogleich einige einfache Eigenschaften, welche hier für den spätern Gebrauch zusammengestellt werden mögen. Wenn α nicht durch p_1 theilbar ist, so hat man $[\alpha; p_1]^2 = \pm 1 \equiv \alpha^{\frac{1}{2}(p-1)}$ (mod. p_1), so dafs es also von dem Werthe des Quadrats $[\alpha; p_1]^2$ abhängt, ob α zu p_1 *quadratischer* Rest ist, oder nicht; und zwar findet der erste oder der zweite Fall Statt, je nachdem in der eben hingeschriebenen Gleichung das obere oder das untere Vorzeichen gilt; ferner ist immer $[\alpha; p_1]^4 = 1$.

Wenn α und β irgend zwei ganze complexe Zahlen sind, so hat man $[\alpha; p_1].[\beta; p_1] = [\alpha\beta; p_1]$, und aus $\alpha \equiv \beta$ (mod. p_1) folgt $[\alpha; p_1] = [\beta; p_1]$. Hiernach ist ferner $[\alpha]^\mu = [\alpha^\mu]$, $[\alpha]^{4\nu+\mu} = [\alpha^\mu]$, wenn μ und ν irgend zwei ganze reelle Zahlen vorstellen; $\frac{1}{[\alpha]} = [\alpha]^3$ u. s. w.

Man kann den Modul p_1 mit einer der complexen Einheiten multipliciren, ohne dafs sich der Werth des Symbols $[\alpha; p_1]$ ändert; denn jede Zahl, welche durch p_1 theilbar ist, ist es auch durch $i^\mu p_1$, und umgekehrt; es ist folglich $[\alpha; p_1] = [\alpha; i^\mu p_1]$. Man darf jedoch nicht auf dieselbe Weise $[\alpha; p_1]$ mit $[i^\mu \alpha; p_1]$ vertauschen; aber es ist $[i^\mu \alpha; p_1] = [i; p_1]^\mu [\alpha; p_1]$. Es ist daher zweckmäfsig, sogleich den Werth von $[i; p_1]$ zu bestimmen. Unmittelbar aus der Definition von $[i; p_1]$ ergiebt sich $[i; p_1] = i^{\frac{1}{4}(p-1)}$. Wählt man, was immer möglich ist, $p_1 = a + bi$ unter den associirten complexen Primzahlen so aus, dafs entweder $a \equiv 1$ (mod. 4), $b \equiv 0$ (mod. 4), oder dafs $a \equiv -1$ (mod. 4), $b \equiv 2$ (mod. 4) ist, so hat man im ersten Falle $a = 4\mu + 1$, $b = 4\nu$, $a^2 \equiv 8\mu + 1$ (mod. 16), $b \equiv 0$ (mod. 16), also $p = a^2 + b^2 \equiv 8\mu + 1$ (mod. 16), $\frac{1}{4}(p-1) \equiv 2\mu \equiv -2\mu \equiv -\frac{1}{2}(a-1)$ (mod. 4), folglich ist

$$[i; p_1] = i^{-\frac{1}{2}(a-1)}.$$

Im zweiten Falle hat man $a = 4\mu - 1$, $b = 4\nu + 2$, $a^2 \equiv -8\mu + 1$ (mod. 16), $b^2 \equiv 4$ (mod. 16), also $p \equiv -8\mu + 5$ (mod. 16), $\frac{1}{4}(p-1) \equiv -2\mu + 1$ (mod. 4), folglich ebenfalls, wie vorhin, $[i; p_1] = i^{-\frac{1}{2}(a-1)}$. Jede ganze complexe Zahl $a + bi$, welche $\equiv 1$ (mod $2 + 2i$), d. h. für welche entweder

$a \equiv 1$ (mod. 4), $b \equiv 0$ (mod. 4), oder $a \equiv -1$, $b \equiv 2$ (mod. 4) ist, heifst *primär*. Ist also $a+bi$ eine primäre complexe Primzahl, so hat man $[i; a+bi] = i^{-\frac{1}{2}(a-1)} = i^{\frac{3}{2}(a-1)}$.

Da nach der Definition $[c+di; a+bi] \equiv (c+di)^{\frac{1}{4}(a^2+b^2-1)}$ (mod. $a+bi$) ist, so folgt, wenn man überall i mit $-i$ vertauscht,

$$[c+di; a+bi]^3 \equiv (c-di)^{\frac{1}{4}(a^2+b^2-1)} \text{ (mod. } a-bi);$$

mithin ist

$$[c-di; a-bi] = [c+di; a+bi]^3.$$

Wenn q eine eingliedrige complexe Primzahl ist, d. h. eine reelle Primzahl, welche, abgesehen vom Zeichen, die Form $4n+3$ hat, und A reell und nicht durch q theilbar ist, so ist immer $[A; q] = 1$; denn da q^2 die Norm von q ist, so hat man $[A; q] \equiv A^{\frac{1}{4}(q^2-1)}$ (mod. q), folglich, weil $\frac{1}{4}(q+1)$ eine ganze Zahl ist,

$$[A; q] \equiv (A^{q-1})^{\frac{1}{4}(q+1)} = 1 \text{ (mod. } q)$$

nach dem *Fermat*schen Satze, also $[A; q] = 1$.

Wenn P irgend eine ganze complexe Zahl ist und ω, ω', ω'', ... sind complexe Primzahlen in beliebiger Anzahl und gleich oder ungleich, so werde die Bedeutung des Zeichens

$$[P; \omega\omega'\omega'' \dots]$$

dahin ausgedehnt, dafs nun darunter das Product

$$[P; \omega][P; \omega'][P; \omega''] \dots$$

zu verstehen sei. Die Bedeutung von $[P; Q]$, wenn P, Q irgend zwei ganze complexe Zahlen sind und Q ungerade ist, ist also dann allgemein festgestellt; der Werth des verallgemeinerten Symbols ist immer noch eine der vier complexen Einheiten, wenn P und Q relative Primzahlen sind; aber Null, wenn P und Q einen gemeinschaftlichen Theiler haben.

Wenn P und Q relative Primzahlen sind, so soll der Exponent derjenigen Potenz von i, welche den Werth von $[P; Q]$ angiebt, der *biquadratische Character* von P in Bezug auf Q heifsen.

In Hinsicht auf die verallgemeinerten Symbole gelten ähnliche Sätze, wie die obigen. Man hat, wenn P, P', Q, Q' irgend vier complexe Zahlen sind und letztere beide ungerade vorausgesetzt werden, wie leicht zu sehen:

$$[P; Q][P'; Q] = [PP'; Q], \quad [P; Q][P; Q'] = [P; QQ'],$$
$$[PP'; QQ'] = [P; Q][P'; Q][P; Q'][P'; Q'],$$
$$[P; i^{\mu} Q] = [P; Q].$$

Aus $P \equiv P'$ (mod. Q) folgt $[P; Q] = [P'; Q]$. Ferner ist

$$[C-Di; A-Bi] = [C+Di; A+Bi]^3.$$

Wenn $A+Bi$ primär, d. h. $\equiv 1$ (mod. $2+2i$) ist, so ist, übereinstimmend mit der oben für primäre Primzahlen bewiesenen Formel,

$$[i; A+Bi] = i^{\frac{3}{2}(A-1)};$$

denn setzt man $A+Bi = (a+bi)(a'+b'i)(a''+b''i)\ldots.$, wo $a+bi$ etc. primäre complexe Primzahlen vorstellen, so ist einerseits

$$[i; A+Bi] = [i; a+bi][i; a'+b'i][i; a''+b''i]\ldots.$$
$$= i^{3(\frac{1}{2}(a-1)+\frac{1}{2}(a'-1)+\frac{1}{2}(a''-1)+\ldots.)};$$

andrerseits aber auch, wie leicht durch das *Kästner*sche Verfahren zu beweisen $\frac{1}{2}(a-1)+\frac{1}{2}(a'-1)+\frac{1}{2}(a''-1)+\cdots \equiv \frac{1}{2}(A-1)$ (mod. 4); folglich u. s. w.

Man bemerke noch die Formel

$$[-1; A+Bi] = (-1)^{\frac{1}{2}(A-1)}.$$

Wir sahen, dafs für eine reelle Primzahl q von der Form $4n+3$, und für eine reelle, nicht durch q theilbare Zahl A, $[A; q] = 1$ ist. Dasselbe gilt auch, wenn q von der Form $4n+1$ ist: denn setzt man in diesem Falle $q = q_1 q_2$, wo q_1 und q_2 conjugirte complexe Primzahlen sind, so erhält man, da A reell ist, also sich nicht ändert, wenn man i mit $-i$ vertauscht, $[A; q_2] = [A; q_1]^3$, also $[A; q_1][A; q_2] = [A; q] = [A; q_1]^4 = 1$. Es ist folglich auch allgemein, wenn A und B irgend zwei reelle ganze Zahlen ohne gemeinschaftliche Theiler vorstellen und B ungerade ist, also A und B aus lauter reellen Primzahlen, theils von der Form $4n+1$, theils von der Form $4n+3$ zusammengesetzt sind.

$$[A; B] = 1.$$

Diese vorläufigen Betrachtungen mufsten angestellt werden, um den Gang der spätern Untersuchungen nicht zu unterbrechen. Ehe wir dieselben verlassen und dem Hauptgegenstande näher kommen, ist aber noch eine Bemerkung nöthig. Wenn p_1 eine complexe Primzahl und α das allgemeine Glied eines vollständigen Restensystems für den Modul p_1 vorstellt, d. h. wenn α eine Reihe von p nach dem mod. p_1 incongruenter Werthe darstellt, so stellt $\beta\alpha$ ebenfalls p nach dem mod. p_1 incongruenter Werthe dar, und ist folglich gleichfalls das allgemeine Glied eines vollständigen Restensystems mod. p_1: vorausgesetzt, dafs β *constant und nicht* durch den Modul p_1 theilbar ist. Hat man also einen Ausdruck, dessen Variabeln und Elemente vollständige Restensysteme nach dem mod. p_1 durchlaufen, und bleiben die einzelnen Glieder dieses Ausdrucks für congruente Werthe der Variabeln unverändert, so kann man jede der Variabeln

resp. mit einer beliebigen constanten, durch p_1 nicht theilbaren ganzen complexen Zahl multipliciren, ohne den Werth des in Rede stehenden Ausdrucks zu verändern.

§. 2.

Betrachtung einer besondern Gattung von Summen.

Es seien $p_1 = a+bi$, $p_2 = a+bi$ zwei conjugirte zweigliedrige complexe Primzahlen; ihre gemeinschaftliche Norm sei die reelle Primzahl p von der Form $4n+1$; $\alpha_1, \alpha_2, \alpha_3, \ldots. \alpha_\mu$ seien *allgemeine Glieder eines vollständigen Restensystems* für den mod. p_1. Man betrachte den Ausdruck

$$\Sigma[\alpha_1][\alpha_2][\alpha_3]\ldots.[\alpha_\mu] = \psi(\mu),$$

in welchem sich die Summationen über die Werthe von $\alpha_1, \alpha_2, \alpha_3, \ldots. \alpha_\mu$ erstrecken, während alle symbolischen Ausdrücke sich auf den Modul p_1 beziehen. Da dieser Ausdruck $\psi(\mu)$ offenbar nichts anders ist, als die μte Potenz von $\Sigma[\alpha_1]$, und da $\Sigma[\alpha_1] = 0$ ist, so hat man

$$\psi(\mu) = 0.$$

Für jedes Glied des Ausdrucks $\psi(\mu)$ mufs die Summe der Elemente

$$\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_\mu = S$$

einem der Glieder des vollständigen Restensystems mod. p_1 congruent sein. Fasset man jedesmal alle diejenigen Glieder von $\psi(\mu)$ zusammen, für welche S demselben Gliede des Restensystems congruent ist, so erhält man $\psi(\mu)$ in p Partialsummen zerfället, von denen wir diejenige, deren sämmtliche Glieder der Bedingung

$$S \equiv \beta \text{ (mod. } p_1)$$

genügen, durch $\psi(\mu, \beta)$ bezeichnen. Man hat für diese Partialsummen, nach der Definition, wenn β das allgemeine Glied eines vollständigen Restensystems mod. p_1 darstellt, zunächst

$$1. \quad \psi(\mu) = \Sigma\psi(\mu, \beta) = 0,$$

wo sich die Summation auf β bezieht.

So oft k nicht durch p_1 theilbar ist, kann man in der Partialsumme

$$\psi(\mu, k) = \underset{\{\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_\mu\equiv k \text{ (mod.} p_1)\}}{\Sigma[\alpha_1][\alpha_2][\alpha_3]\ldots.[\alpha_\mu]}$$

$\alpha_1, \alpha_2, \alpha_3, \ldots. \alpha_\mu$ resp. durch $k\beta_1, k\beta_2, k\beta_3, \ldots. k\beta_\mu$ ersetzen und die verschiedenen β, so weit es sich mit den übrigen Bedingungen verträgt, wiederum vollständige Restensysteme mod. p_1 durchlaufen lassen; welches

$$\underset{\{k\beta_1+k\beta_2+k\beta_3+\cdots+k\beta_\mu\equiv k \text{ (mod.} p_1)\}}{\Sigma[k\beta_1][k\beta_2][k\beta_3]\ldots.[k\beta_\mu]}$$

giebt. Schafft man die Bedingungscongruenz durch die Division mit k weg und zieht aus dem allgemeinen Gliede der Summe den Factor $[k]^\mu$ heraus, so ergiebt sich

$$[k]^\mu \Sigma[\beta_1][\beta_2][\beta_3]\ldots[\beta_\mu],$$
$$\{\beta_1+\beta_2+\beta_3+\cdots+\beta_\mu\equiv 1 \pmod{p_1}\},$$

folglich, sobald k nicht durch p_1 theilbar ist,

$$2.\qquad \psi(\mu,k) = [k]^\mu \psi(\mu,1).$$

Wegen (1.) folgt hieraus $\psi(\mu,0)+\Sigma[\beta]^\mu\psi(\mu,1)=0$ und

$$3.\qquad \psi(\mu,0) = -(p-1)\psi(\mu,1),\quad \text{oder}\quad =0,$$

je nachdem μ von der Form $4n$, oder nicht von dieser Form ist.

Zur näheren Bestimmung des Werths der Summen $\psi(\mu,k)$ bilde man die Recursionsformel

$$4.\qquad \psi(\mu,k) = \Sigma[\alpha]\psi(\mu-1,k-\alpha),$$

in welcher α das allgemeine Glied eines vollständigen Restensystems mod. p_1 ist. Die Richtigkeit derselben erhellet aus der Gleichung

$$\psi(\mu,k) = \Sigma[\alpha_\mu]\times[\alpha_1][\alpha_2][\alpha_3]\ldots[\alpha_{\mu-1}]$$
$$\{\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{\mu-1}\equiv k-\alpha_\mu \pmod{p_1}\}.$$

Die Recursionsformel liefert zunächst für $\mu=4n$,

$$\psi(4n,0) = \Sigma[\alpha]\psi(4n-1,-\alpha) = \psi(4n-1,1)\Sigma[\alpha][-\alpha]^3$$

nach (2.), folglich

$$\psi(4n,0) = [-1]^3(p-1)\psi(4n-1,1) = (p-1)[-1]\psi(4n-1,1),$$

mithin auch nach (3.)

$$\psi(4n,1) = -[-1]\psi(4n-1,1).$$

Die Recursionsformel giebt ferner, mit Benutzung von (2.) und (3.),

$$\psi(4n+1,1) = \Sigma[\alpha]\psi(4n,1-\alpha) = \psi(4n,0)+\Sigma[\alpha]\psi(4n,1)-\psi(4n,1)$$
$$= -p\,\psi(4n,1).$$

Endlich erhält man für $\mu=4n+2$, $4n+3$,

$$\psi(4n+2,1) = \Sigma[\alpha]\psi(4n+1,1-\alpha) = \psi(4n+1,1)\Sigma[\alpha][1-\alpha],$$
$$\psi(4n+3,1) = \Sigma[\alpha]\psi(4n+2,1-\alpha) = \psi(4n+2,1)\Sigma[\alpha][1-\alpha]^2.$$

Setzt man der Kürze wegen

$$5.\qquad \Sigma[\alpha][1-\alpha] = P,\quad \Sigma[\alpha][1-\alpha]^2 = Q$$

und $\psi(\mu,1)=\chi(\mu)$, so ergiebt sich

$$\chi(1) = [1] = 1,\quad \chi(2) = P,\quad \chi(3) = PQ,\quad \chi(4) = -[-1]PQ,$$
$$\chi(5) = p[-1]PQ,\quad \chi(6) = p[-1]P^2Q,\quad \chi(7) = p[-1]P^2Q^2,$$
$$\chi(8) = -p[-1]^2P^2Q^2,\quad \text{u. s. w.,}$$

folglich allgemein

$$6.\quad \begin{cases} \psi(4n+1,1) = p^n[-1]^n P^n Q^n, \\ \psi(4n+2,1) = p^n[-1]^n P^{n+1} Q^n, \\ \psi(4n+3,1) = p^n[-1]^n P^{n+1} Q^{n+1}, \\ \psi(4n+4,1) = -p^n[-1]^{n+1} P^{n+1} Q^{n+1}, \end{cases}$$

wo n die Null oder irgend eine ganze positive Zahl bezeichnet. Die Werthe von $\psi(\mu,\beta)$, wenn β von 1 verschieden ist, findet man hiernach sogleich mit Hülfe von (2.) und (3.).

Wir wollen noch die Anzahl der von 0 verschiedenen Glieder suchen, welche die Summe $\psi(\mu,k)$ enthalten. Bezeichnet man diese Anzahl durch $Z(\mu,k)$, so ist offenbar, wenn k nicht durch p_1 theilbar ist, $Z(\mu,k)=(\mu,1)$, folglich, wie leicht zu sehen,

$$Z(\mu+1,1) = Z(\mu,0)+Z(\mu,2)+Z(\mu,3)+\cdots+Z(\mu,p-1)$$
$$= Z(\mu,0)+(p-2)Z(\mu,1), \quad \text{und}$$
$$Z(\mu+1,0) = Z(\mu,1)+Z(\mu,2)+\cdots+Z(\mu,p-1) = (p-1)Z(\mu,1).$$

Hieraus ergiebt sich $Z(1,0)=0$, $Z(1,1)=1$, $Z(2,0)=p-1$, $Z(2,1)=p-2$, $Z(3,0)=(p-1)(p-2)$, $Z(3,1)=(p-1)+(p-2)^2$, $Z(4,0)=(p-1)^2+(p-1)(p-2)^2$, $Z(4,1)=2(p-1)(p-2)+(p-2)^3$ u. s. w. Es hat keine Schwierigkeit, durch Auflösung der Differenzengleichung

$$Z(\mu,1) = (p-2)Z(\mu-1,1)+(p-1)Z(\mu-2,1)$$

den Werth von $Z(\mu,1)$ und hieraus auch den von $Z(\mu,0)$ allgemein zu finden. In der That ergiebt sich $Z(\mu,1)=\frac{1}{p}((p-1)^\mu-(-1)^\mu)$.

§. 3.

Über den Rest der Summen $\psi(q,1)$ (mod. q).

Es ist für das Folgende nöthig, den Rest zu bestimmen, welchen für eine reelle Primzahl q die Summe $\psi(q,1)$ läfst, wenn man sie durch q dividirt. Diese Division läfst sich in der That allgemein verrichten. Es sei q eine von p verschiedene reelle und ungerade (positive) Primzahl. Untersuchen wir zunächst, ob in der Summe

$$\psi(q,1) = \Sigma[\alpha_1][\alpha_2][\alpha_3]\dots[\alpha_q]$$
$$\{\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_q\equiv 1 \pmod{p_1}\}$$

Glieder vorkommen können, für welche $\alpha_1=\alpha_2=\cdots=\alpha_q$, nemlich alle Elemente, einander gleich sind. Für alle Glieder, welche dieser letztern Bedingung genügen, ist auch $q\alpha_1\equiv 1 \pmod{p_1}$: eine Congruenz, welcher immer ein, aber nur ein einziger Werth von α_1 genügt. Wird dieser Werth durch r bezeichnet, so dafs $qr\equiv 1 \pmod{p_1}$ ist, so kommt in $\psi(q,1)$ das Glied

$[r][r][r]\dots.[r]=[r]^q=[q]^{3q}$ vor (und nur dieses), für welches alle Elemente einander gleich sind. Alle Glieder erscheinen in Gruppen zu je q; denn. ist

$$[\alpha_1][\alpha_2][\alpha_3]\dots.[\alpha_{q-2}][\alpha_{q-1}][\alpha_q]$$

irgend eines von diesen Gliedern, für welches also die beiden Bedingungen erfüllt werden, dafs die Summe der Elemente $\equiv 1 \pmod{p_1}$ ist, und dafs nicht alle Elemente einander gleich sind, so gesellen sich zu demselben noch die $q-1$ folgenden Glieder:

$$\begin{array}{l} [\alpha_2][\alpha_3][\alpha_4]\dots.[\alpha_{q-1}][\alpha_q][\alpha_1], \\ [\alpha_3][\alpha_4][\alpha_5]\dots.[\alpha_q][\alpha_1][\alpha_2], \\ [\alpha_4][\alpha_5][\alpha_6]\dots.[\alpha_1][\alpha_2][\alpha_3], \\ \dots\dots\dots\dots\dots\dots\dots \\ [\alpha_q][\alpha_1][\alpha_2]\dots.[\alpha_{q-3}][\alpha_{q-2}][\alpha_{q-1}], \end{array}$$

welche aus jenem durch eine *cyclische* oder *ähnliche* Permutation der Elemente entstehen. Diese q Glieder kommen alle in der Summe $\psi(q,1)$ wirklich vor; keines von ihnen ist mit einem andern identisch, d. h. *keines* von ihnen ist durch ein anderes *schon mit gesetzt:* denn einerseits genügen alle diese Glieder den erforderlichen Bedingungen, und andrerseits können nie zwei ähnliche Permutationen identisch sein, weil q eine Primzahl ist, und nicht alle Elemente einander gleich sind. Je q Glieder der Differenz $\psi(q,1)-[q]^{3q}$, welche durch eine cyclische Permutation der Elemente aus einander entstehen, lassen sich also zu einer Gruppe vereinigen; und da jedesmal alle Glieder einer und derselben Gruppe einander gleich sind, so läfst sich diese Differenz auf die Form qU bringen, während U eine ganze complexe Zahl ist; nemlich eine Summe von complexen Einheiten, welche man erhält, wenn man in der Summe

$\Sigma[\alpha_1][\alpha_2]\dots.[\alpha_q]$ $\{\alpha_1+\alpha_2+\dots+\alpha_q\equiv 1 \pmod{p_1}\}$ dasjenige Glied *ausschliefst,* für welches alle Elemente einander gleich sind, und dann unter den übrigen Gliedern von je q Gliedern, welche durch die cyclische Permutation der Elemente auseinander entstehen, jedesmal nur ein *einziges* nimmt. Wenn man also die Summe $\psi(q,1)$ durch q dividirt, so erhält man den Quotienten U und den Rest $[q]^{3q}$ oder $[q;p_1]^{3q}$, d. h.

$$\psi(q,1) = qU+[q,p_1]^{3q}.$$

Es lassen sich auch a priori die Reste von $\psi(2,1)$ und $\psi(4,1)$ nach dem Modul $2+2i$ bestimmen. Es ist nemlich $\psi(2,1)=[2][p-1]+3[p-2]+\dots$ $\dots+[p-1][2]=2.\{[2][-1]+[3][-2]+\dots+[\frac{1}{2}(p-1)][-\frac{1}{2}(p-3)]\}+[\frac{1}{2}(p+1)]^2$. Der Ausdruck innerhalb der Parenthese $\{\}$ ist eine Summe von $\frac{1}{2}(p-3)$ com-

plexen Einheiten. Da nun $1-1$, $1-i$, $1+1$, und $1+i$ alle vier durch $1+i$ theilbar sind, also jede complexe Einheit $\equiv 1$ (mod. $1+i$) ist, so ist jener Ausdruck in der Parenthese $\equiv \frac{1}{2}(p-3)$ (mod. $1+i$), folglich $\psi(2,1) \equiv 2.\frac{1}{2}(p-3)+[\frac{1}{2}(p+1)]^2$ (mod. $2+2i$). Aber $[\frac{1}{2}(p+1)] = \frac{[1]}{[2]} = [2]^3 = [1+i]^6[-i]^3$, und $p-3 \equiv -2$ (mod. 4), folglich $\psi(2,1) \equiv -2+[-1] \equiv \pm 2+[-1] \equiv -[-1]$ (mod. $2+2i$).

In der Summe $\psi(4,1) = \sum_{\{\alpha_1+\alpha_2+\alpha_3+\alpha_4 \equiv 1 \, (\text{mod.} p_1)\}} [\alpha_1][\alpha_2][\alpha_3][\alpha_4]$ findet sich ein Glied, für welches alle Elemente einander gleich sind, indem die Congruenz $4\alpha_1 \equiv 1$ (mod. p_1) genau eine Auflösung zuläfst; der Werth dieses Gliedes ist $[\alpha_1]^4 = 1$. Alle übrigen Glieder kommen paarweise vor, indem von je vier Gliedern, wie

$$\begin{gathered}
[\alpha_1][\alpha_2][\alpha_3][\alpha_4], \\
[\alpha_2][\alpha_3][\alpha_4][\alpha_1], \\
[\alpha_3][\alpha_4][\alpha_1][\alpha_2], \\
[\alpha_4][\alpha_1][\alpha_2][\alpha_3],
\end{gathered}$$

für welche nicht alle Elemente einander gleich sind, entweder alle vier verschieden, oder doch nur höchstens zwei und zwei identisch sein können. Die Summe $\psi(4,1)$ läfst sich also auf die Form $2V+1$ bringen, wo V eine ganze complexe Zahl ist, die $\frac{1}{2}(Z(4,1)-1) = (p-1)(p-2)+\frac{1}{2}((p-2)^3-1)$ complexe Einheiten enthält. Es ist folglich, da jede complexe Einheit $\equiv 1$ (mod. $1+i$) ist, $V = (p-1)(p-2)+\frac{1}{2}((p-2)^3-1)$ (mod. $1+i$), also $\psi(4,1) \equiv 2(p-1)(p-2)+(p-2)^3$ (mod. $2+2i$) $\equiv (p-2)^3 \equiv (-1)^3 \equiv -1$ (mod. $2+2i$).

Auf einen Umstand ist hier besonders zu sehen, der sogleich eine wichtige Anwendung finden wird. Es ist der, dafs für eine von p verschiedene ungerade Primzahl q die complexe Zahl $\psi(q,1)$ nicht durch q theilbar sein kann; denn $\psi(q,1)$ läfst, durch q dividirt, den Rest $[q]^{3q}$, welcher eine complexe Einheit ist, also nicht durch q theilbar sein kann; auch kann für den Fall $q \equiv 1$ (mod. 4), $\psi(q,1)$ nicht durch einen der beiden complexen Primfactoren von q theilbar sein, weil sonst auch die complexe Einheit $[q]^{3q}$ durch dieselbe complexe Primzahl theilbar wäre; was unmöglich ist. Auf dieselbe Weise können $\psi(2,1)$ und $\psi(4,1)$ nicht durch $1+i$ theilbar sein. Es folgt hieraus noch, dafs die Norm von $\psi(q,1)$ in keinem Falle durch q, und dafs die Normen von $\psi(2,1)$ und $\psi(4,1)$ nicht durch 2 theilbar sind.

§. 4.

Lemma. „Wenn α das allgemeine Glied eines vollständigen Restensystems mod. p_1 darstellt, und m, n zwei positive ganze Zahlen >0 und $<p-1$ sind, so ist

$$\Sigma\alpha^m(1-\alpha)^n \equiv 0 \quad \text{oder} \quad \equiv -(-1)^{p-1-m}n_{p-1-m} \pmod{p_1},$$

je nachdem $m+n<p-1$ oder $m+n \geqq p-1$ ist. Das Zeichen n_τ bedeutet für den Augenblick den Binomialcoëfficienten $\frac{n(n-1)\dots(n-\tau+1)}{1.2\dots\tau}$ ".

Beweis. Der Werth der Summe, deren Rest nach dem mod. p_1 zu finden ist, sei T. Da es, der Natur der Frage gemäfs, offenbar ganz gleichgültig ist, welches Restensystem man α durchlaufen läfst, und da man das durch p_1 theilbare Glied ebensowohl weglassen als beibehalten kann, so ist es erlaubt, eine primitive Wurzel γ für den mod. p_1 zu wählen und dem Summationsbuchstaben α die Werthe

$$1, \ \gamma, \ \gamma^2, \ \gamma^3, \ \dots \ \gamma^{p-2}$$

zu geben, welches

$$T \equiv \sum_{\sigma=0}^{\sigma=p-2} \gamma^{\sigma m}(1-\gamma^\sigma)^n \pmod{p_1}$$

giebt. Entwickelt man die Potenz $(1-\gamma^\sigma)^n$ nach dem Binomialtheorem, so findet sich

$$(1-\gamma^\sigma)^n = \sum_{\tau=0}^{\tau=n} n_\tau(-1)^\tau\gamma^{\sigma\tau},$$

also

$$T \equiv \sum_{\sigma=0}^{\sigma=p-2}\sum_{\tau=0}^{\tau=n} n_\tau(-1)^\tau\gamma^{\sigma(m+\tau)} \pmod{p_1}.$$

Es ist aber

$$\sum_{\sigma=0}^{\sigma=p-2}\gamma^{\sigma(m+\tau)} = \frac{1-\gamma^{(p-1)(m+\tau)}}{1-\gamma^{m+\tau}} \equiv 0 \pmod{p_1},$$

wenn $m+\tau$ *nicht* durch $p-1$ theilbar ist; dagegen ist

$$\sum_{\sigma=0}^{\sigma=p-2}\gamma^{\sigma(m+\tau)} \equiv 1+1+\dots+1 \equiv p-1 \equiv -1 \pmod{p_1},$$

wenn $m+\tau$ durch $p-1$ theilbar ist.

Der gröfste Werth, welchen $m+\tau$ erhalten kann, ist $m+n$. Ist also $m+n$ kleiner als $p-1$, so giebt es keinen einzigen durch $p-1$ theilbaren Werth von $m+\tau$, und es ist in diesem Falle T einer Summe von $n+1$ Nullen congruent; also selbst $\equiv 0 \pmod{p_1}$. Ist dagegen $m+n \geqq p-1$, so giebt es einen Werth von $m+\tau$, welcher durch $p-1$ theilbar ist, nemlich für $m+\tau = p-1$, also für $\tau=p-1-m$, und man erhält

$$T \equiv -n_{p-1-m}(-1)^{p-1-m} \pmod{p_1}: \quad \text{was zu beweisen war.}$$

§. 5.

Bestimmung von P und Q.

Die Werthe der Summen $\psi(\mu, 1)$ wurden oben durch die beiden Summen P und Q ausgedrückt. Wir gehen jetzt zur vollständigen Bestimmung der beiden letztern über. Da

$$[\alpha] \equiv \alpha^{\frac{1}{4}(p-1)} \pmod{p_1}, \qquad [1-\alpha] \equiv (1-\alpha)^{\frac{1}{4}(p-1)} \pmod{p_1}$$

ist, so hat man

$$P = \Sigma[\alpha][1-\alpha] \equiv \Sigma\alpha^{\frac{1}{4}(p-1)}(1-\alpha)^{\frac{1}{4}(p-1)} \pmod{p_1},$$
$$Q = \Sigma[\alpha][1-\alpha]^2 \equiv \Sigma\alpha^{\frac{1}{4}(p-1)}(1-\alpha)^{\frac{1}{2}(p-1)} \pmod{p_1}.$$

Da nun $\frac{1}{4}(p-1)+\frac{1}{4}(p-1)=\frac{1}{2}(p-1)<p-1$ und $\frac{1}{4}(p-1)+\frac{1}{2}(p-1) = \frac{3}{4}(p-1)$ ebenfalls $<p-1$ ist, so sind nach dem eben bewiesenen Lemma die beiden Summen, denen P und Q congruent sind, durch p_1 theilbar; folglich sind auch P und Q durch p_1 theilbar und es ist

$$P \equiv 0 \pmod{p_1}, \qquad Q \equiv 0 \pmod{p_1}.$$

Dies ist der erste Schritt zur Bestimmung von P und Q.

Suchen wir jetzt die Normen von P und Q zu finden. Diese Normen können durch keine von p verschiedene Primzahl theilbar sein; denn wären z. B. eine der beiden Normen, oder beide, durch die von p verschiedene ungerade Primzahl $q>1$ theilbar, so müfste auch $N(\psi(q, 1))$, welches nach §. 2. die beiden Factoren $N(P)$ und $N(Q)$ enthält, durch q theilbar sein; was nicht möglich ist (§. 3. am Schlusse): und wäre $N(P)$ oder $N(Q)$ durch 2 theilbar, so wäre auch $N(\psi(4, 1)) = N(P)N(Q)$ durch 2 theilbar; was ebenfalls nicht sein kann (§. 3.).

Andrerseits sind P und Q durch p_1, also ihre Normen durch p theilbar; es kann daher $N(P)$ sowohl als $N(Q)$ nur eine Potenz von p sein, mit einem Exponenten $\geqq 1$. Aber P und Q bestehen beide aus $p-2$ complexen Einheiten; und da nun die Norm jeder complexen Einheit $= 1$ ist, so ist $N(P) \leqq (p-2)^2$; $N(Q) \leqq (p-2)^2$ *); der Exponent p, von welchem so eben die Rede war, kann also nicht die Einheit übersteigen, und man hat daher $N(P)=p$, $N(Q)=p$.

Da die eben gemachten Schlüsse etwas eigenthümlich sind, so wird es gut sein, den Gang derselben kurz zu wiederholen. Wir zeigten zuerst, dafs P und Q durch p_1 theilbar sind; und zwar geschah dies, indem wir Summen

*) Wenn u und u' irgend zwei complexe Zahlen sind, so ist, wie aus den Elementen der Algebra bekannt, $\sqrt{(N(u+u'))} \leqq \sqrt{(N(u))}+\sqrt{(N(u'))}$, folglich auch allgemein $\sqrt{(N(u+u'+u''+\ldots))} \leqq \sqrt{(N(u))}+\sqrt{(N(u'))}+\sqrt{(N(u''))}+\ldots$; woraus das im Texte Behauptete folgt.

aufstellten, welche jenen nach dem mod. p_1 congruent, ihrerseits aber durch p_1 theilbar sind: die Normen von P und Q sind also durch p theilbar; sie können aber durch keine andere Primzahl theilbar sein, weil sonst andere Summen, welche jene als Factoren enthalten, durch dieselbe Primzahl theilbar wären, wovon wir aber bereits das Gegentheil wissen (§. 3.); es bleibt also für unsere Normen nichts anders übrig, als eine Potenz von p; und diese kann nicht höher als die erste sein, weil man eine Grenze angeben kann, welche $N(P)$ und $N(Q)$ nicht überschreiten, und welche Grenze noch unter p^2 liegt.

Da nun also P und Q durch p_1 theilbar, und ihre Normen $=p$ sind, so müssen P und Q nothwendig entweder $=p_1$, oder doch zu p_1 associirt sein. Es wird in dieser Hinsicht kein Zweifel mehr Statt finden, sobald sich der Rest von P und Q nach dem Modul $2+2i$ bestimmen läfst. Man hat nach §. 3. $\psi(2,1)=P\equiv-[-1]$ (mod. $2+2i$), $\psi(4,1)=-[-1]PQ\equiv-1$ (mod. $2+2i$), folglich auch, substituendo, $Q\equiv-1$ (mod. $2+2i$), also

$$P\equiv-[-1],\quad Q\equiv-1 \pmod{2+2i}.$$

Da bisher über die Wahl von p_1 unter den associirten Zahlen noch nichts festgesetzt ist, so wollen wir übereinkommen, p_1 primär, d. h. $\equiv 1$ (mod. $2+2i$) anzunehmen. Unter dieser Voraussetzung findet sich

$$P=-[-1]p_1 \quad\text{und}\quad Q=-p_1,$$

so dafs nun die Werthe von P und Q vollständig bestimmt sind.

Substituirt man endlich die eben gefundenen Werthe von P und Q in den Formeln §. 2., so kommt, wegen $[-1]^n P^n Q^n=p_1^{2n}$,

$$\begin{aligned}\psi(4n+1,1) &= +p^n p_1^{2n},\\ \psi(4n+2,1) &= -[-1]p^n p_1^{2n+1},\\ \psi(4n+3,1) &= +[-1]p^n p_1^{2n+2},\\ \psi(4n+4,1) &= -p^n p_1^{2n+2};\end{aligned}$$

und diese Formeln erfordern, dafs p_1 primär, d. h. $\equiv 1$ (mod. $2+2i$) genommen wird.

Zusatz. Da $\Sigma[\alpha][1-\alpha]=-[-1]p_1=-(-1)^{\frac{1}{4}(p-1)}p_1$, so ist auch $\Sigma[\alpha]^3[1-\alpha]^3=-(-1)^{\frac{1}{4}(p-1)}p_2$. Aber $\Sigma[\alpha]^3[1-\alpha]^3\equiv\Sigma\alpha^{\frac{3}{4}(p-1)}(1-\alpha)^{\frac{3}{4}(p-1)}$ (mod. p_1); und da in dieser letztern Summe, wenn man der Kürze wegen $\frac{1}{4}(p-1)=r$ setzt, mit §. 4. verglichen, $m=3r$, $n=3r$, also $m+n=6r>p-1$ und $p-1-m=r$ ist, so hat man nach dem Lemma (§. 4.):

$$-(-1)^{\frac{1}{4}(p-1)}p_2\equiv-\frac{3r.(3r-1).(3r-2)\ldots.(2r+1)}{1\,.\,2\,.\,3\,\ldots.\,r}(-1)^r,\ \text{folglich}$$

$$p_2\equiv\frac{3r.(3r-1).(3r-2)\ldots.(2r+1)}{1\,.\,2\,.\,3\,\ldots.\,r}\pmod{p_1}.$$

Ferner haben wir $\Sigma[\alpha][1-\alpha]^2 = -p_1$ gefunden, folglich ist auch $\Sigma[\alpha]^3[1-\alpha]^2 = -p_2 \equiv \Sigma\alpha^{\frac{3}{4}(p-1)}(1-\alpha)^{\frac{1}{2}(p-1)}$ (mod. p_1). Hier ist $m=3r$, $n=2r$, $m+n=5r>p-1$, $p-1-m=r$, folglich nach §. 4.

$$p_2 \equiv (-1)^{\frac{1}{4}(p-1)} \frac{2r.\,2r-1.\,2r-2\ldots.r+1}{1\,.\;2\;.\;3\;\ldots.\;r} \pmod{p_1}.$$

Das eine Resultat ist übrigens eine unmittelbare Folge des andern.

§. 6.

Das Fundamentaltheorem in seiner einfachsten Gestalt.

Wir kennen jetzt für jede von p verschiedene reelle ungerade Primzahl q die Werthe der Summen $\psi(q,1)$ und auch ihre Reste nach dem Modul q. Durch Verbindung dieser beiden Resultate ergiebt sich Folgendes.

A. Wenn q eine Primzahl $4n+3$ ist, so hat man nach (§. 5.) $\psi(q,1)=[-1]p^{\frac{1}{4}(q-3)}p_1^{\frac{1}{2}(q+1)}$, und nach (§. 3.) $\psi(q,1)\equiv[q;p_1$ (mod. q), weil $3q\equiv 1$ (mod. 4) ist; also erhält man

1. $\quad [-1]\,p^{\frac{1}{4}(q-3)}p_1^{\frac{1}{2}(q+1)} \equiv [q;p_1] \pmod{q}.$

B. Ist zweitens q von der Form $4n+1$, so ist nach (§. 5.) $\psi(q,1)=p^{\frac{1}{4}(q-1)}p_1^{\frac{1}{2}(q-1)}$, und nach (§. 3.) $\psi(q,1)\equiv[q;p_1]^3$ (mod. q), weil jetzt $3q\equiv 3$ (mod. 4); also ist

2. $\quad p^{\frac{1}{4}(q-1)}p_1^{\frac{1}{2}(q-1)} \equiv [q;p_1]^3 \pmod{q},$

und in beiden Formeln (1.) und (2.) läfst sich der Quotient der Division durch q nach (§. 3.) allgemein hinschreiben. Ein Beispiel einer solchen allgemein ausführbaren Division, bei welcher man die numerischen Werthe des Dividendus und Divisors nicht zu kennen braucht, scheint ziemlich merkwürdig zu sein, und bekräftigt die Richtigkeit des Resultats aufs schärfste.

C. Wenn wiederum $q=4n+3$ ist, so folgt aus (1.), wenn man beide Theile zur Potenz $\frac{1}{2}(q-1)$ erhebt, und bedenkt, dafs $\frac{1}{2}(q-1)$ ungerade, also $[-1]^{\frac{1}{2}(q-1)}=[-1]$ ist,

3. $\quad [-1]\,p^{\frac{1}{4}(q-3).\frac{1}{2}(q-1)}p_1^{\frac{1}{4}(q^2-1)} \equiv [q,p_1]^{\frac{1}{2}(q-1)} \pmod{q}.$

Nun ist, wenn man sich des aus der Theorie der quadratischen Reste bekannten Legendreschen Zeichens bedient:

$$p^{\frac{1}{2}(q-1)} \equiv \left(\frac{p}{q}\right) \pmod{q}.$$

Da $p\equiv 1$ (mod. 4), so ist $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ (Fundamentaltheorem für die quadratischen Reste); ferner $\left(\frac{q}{p}\right)\equiv q^{\frac{1}{2}(p-1)}$ (mod. p), also auch $\left(\frac{q}{p}\right)\equiv q^{\frac{1}{2}(p-1)}$ (mod. p_1),

folglich $\left(\frac{q}{p}\right) = [q^2; p_1] = [q, p_1]^2$, mithin $\left(\frac{p}{q}\right) = [q, p_1]^2$ und

$$p^{\frac{1}{4}(q-3) \cdot \frac{1}{2}(q-1)} \equiv [q; q_1]^{\frac{1}{2}(q-3)} \pmod{q}.$$

Substituirt man diesen Werth in die Congruenz (3.) und hebt auf beiden Seiten den gemeinschaftlichen Factor $[q; p]^{\frac{1}{2}(q-3)}$ heraus, so kommt

$$[-1]\, p_1^{\frac{1}{4}(q^2-1)} \equiv [q; p] \pmod{q}, \text{ oder}$$

$$4. \quad p_1^{\frac{1}{4}(q^2-1)} \equiv [-q, p_1] \pmod{\pm q} \text{ *)}.$$

Da nun q^2 die Norm von der reellen und zugleich complexen Primzahl $-q$ ist, und da wir diejenige complexe Einheit, welcher $p_1^{\frac{1}{4}(q^2-1)}$ (mod. $-q$) congruent ist, durch $[p_1; -q]$ bezeichnen, so haben wir aus (4.) die merkwürdige Reciprocitätsformel

$$5. \quad [p_1; -q] = [-q; p_1].$$

„Wenn p_1 eine primäre zweigliedrige Primzahl mit der Norm p, „und $-q$ eine primäre eingliedrige Primzahl ist, d. h. eine reelle „Primzahl, welche, abgesehn vom Zeichen, die Form $4n+3$ hat, so „ist der Rest der Potenz $p_1^{\frac{1}{4}(q^2-1)}$ durch $-q$ derselbe, wie der Rest „der Potenz $(-q)^{\frac{1}{4}(p-1)}$ durch p_1."

D. Wenn wieder wie in (***B.***) q die Form $4n+1$ hat, und q_1 und q_2 die beiden primären Primfactoren von q sind, so giebt die Congruenz (2.)

$$(p p_1^2)^{\frac{1}{4}(q-1)} \equiv [q; p_1]^3 \pmod{q_1},$$

folglich, da q die Norm von q ist,

$$[p p_2^2; q_1] = [q; p_1]^3, \quad \text{oder} \quad [p_1^3 p_2; q_1] = [q; q_1]^3$$

und, wenn man beide Seiten zum Cubus erhebt,

$$6. \quad [p_1 p_2^3; q_1] = [q; p_1].$$

Aber nach einer in §. 1. gemachten Bemerkung hat man, da p_1 mit p_2, q_1 mit q_2 *conjugirt* ist,

$$[p_2^3; q_1] = [p_2; q_1]^3 = [p_1, q_2],$$

folglich wegen (6.)

$$[p_1; q_1][p_1; q_2] = [q; p_1], \quad \text{oder}$$

$$7. \quad [p_1; q] = [q; p_1].$$

Dieses Resultat ist demjenigen, welches wir vorhin in (5.) für eine reelle Primzahl $4n+3$ fanden, vollkommen analog. Welche reelle, von p verschie-

---

*) Diese Formel (4.) läfst sich auf noch viel einfacherem Wege aus (1.) ableiten. Der Gleichung (1.) kann man die Form $p_1^{\frac{1}{4}(3q-1)} p_2^{\frac{1}{4}(q-3)} \equiv [-q, p_1] \pmod{q}$ geben; erwägt man nun, dafs $p_2 \equiv p_1^q \pmod{q}$ ist, so erhält man hieraus unmittelbar durch Substitution von p_1^q an die Stelle von p_2 die Gleichung (4.).

dene primäre Primzahl also auch l bedeuten mag, sie mag positiv und von der Form $4n+1$, oder negativ und abgesehn vom Zeichen von der Form $4n+3$ sein: immer ist

$$8. \quad [p_1; l] = [l; p_1].$$

§. 7.

Das Fundamentaltheorem, wenn die eine Zahl *reell* ist.

Wir gehen zu der Verallgemeinerung und Ergänzung der in dem vorigen Paragraph gefundenen Resultate über. Jede primäre reelle Zahl L, d. h. jede reelle Zahl L, welche mit ihrem Zeichen $\equiv 1 \pmod{4}$ ist, läfst sich in ein Product von reellen Primzahlen $l_1, l_2, l_3, l_4, \ldots$ zerlegen, welche theils positiv und $\equiv 1$ (mod. 4.), theils negativ und, abgesehn vom Zeichen, $\equiv 3$ (mod. 4) sind, und man hat dann

$$[p_1; L] = \Pi[p_1; l], \quad [L; p_1] = \Pi[l; p_1],$$

wo sich die Multiplicationszeichen Π auf die verschiedenen l erstrecken. Aber nach dem vorigen Paragraphen ist für jedes der eben definirten l, welche wir sämmtlich von p verschieden voraussetzen, $[p_1; l] = [l; p_1]$, mithin auch $\Pi[p_1; l] = \Pi[l; p_1]$, d. h.

$$[p_1; L] = [L; p_1].$$

Die Gleichung $[t; L] = [L; t]$ gilt also, wenn t eine primäre zweigliedrige complexe Primzahl und L eine beliebige primäre ***reelle*** Zahl ist, in welche t nicht aufgeht; sie gilt aber auch ferner, wenn t eine primäre eingliedrige Primzahl ist, d. h. eine reelle Primzahl $4n+3$, mit dem negativen Zeichen genommen. In der That, in diesem zweiten Falle hat man schon nach (§. 1.) $[t; L] = 1$, $[L; t] = 1$, also gewifs $[t; L] = [L; t]$.

Jede denkbare primäre complexe Zahl T läfst sich auf die Form $t_1, t_2, t_3, t_4, \ldots$ bringen, wo t_1 etc. theils primäre zweigliedrige, theils primäre eingliedrige complexe Primzahlen vorstellen; man kann also

$$[T; L] = \Pi[t; L] \quad \text{und} \quad [L, T] = \Pi[L; t]$$

setzen, und da nach dem eben Bewiesenen $[t; L] = [L; t]$ ist, so folgt

$$[T; L] = [L; T],$$

wenn T und L keinen gemeinschaftlichen Factor haben.

„Wenn also T irgend eine primäre complexe Zahl, L irgend eine „primäre reelle Zahl vorstellt, welche zu jener relative Primzahl „ist, so hat man immer $[T; L] = [L; T]$.“

Es ist kaum nöthig, zu bemerken, dafs diese Gleichung auch noch gilt, wenn T und L einen gemeinschaftlichen Factor haben; denn in diesem Falle ist $[T; L] = 0$ und $[L; T] = 0$.

§. 8.

Das allgemeinste Fundamentaltheorem.

Es bleiben noch zwei zweigliedrige Zahlen mit einander zu vergleichen. Es seien $A+Bi$ und $C+Di$ irgend zwei primäre complexe Zahlen (den Fall $B=0$ oder $D=0$ nicht ausgeschlossen) ohne gemeinschaftlichen Theiler; m sei der gröfste primäre gemeinschaftliche Theiler von A und B, n der gröfste primäre gemeinschaftliche Theiler von C und D, so dafs man

$$A+Bi = m(a+bi), \quad C+Di = n(c+di)$$

setzen kann, wo a zu b und c zu d relative Primzahl ist, während $m \equiv 1$, $n \equiv 1 \pmod{4}$, $a+bi \equiv 1$, $c+di \equiv 1 \pmod{2+2i}$ ist. Es ist zunächst

$$[A+Bi; C+Di] = [m; n][m; c+di][a+bi; n][a+bi; c+di],$$
$$[C+Di; A+Bi] = [n; m][n; a+bi][c+di; m][c+di; a+bi].$$

Da nun nach dem bereits Bewiesenen $[m; n] = [n; m]$, $[m; c+di] = [c+di; m]$ und $[a+bi; n] = [n; a+bi]$ ist, so kommt Alles auf die Vergleichung von $[a+bi; c+di]$ mit $[c+di; a+bi]$ an. Hierzu wird die Betrachtung der identischen Gleichung

$$1. \quad c(a+bi) = ac+bd+bi(c+di)$$

führen. Es folgt aus dieser Gleichung $c(a+bi) \equiv ac+bd \pmod{c+di}$, und da c mit d, also auch mit $c+di$ und $a+bi$ mit $c+di$ keinen gemeinschaftlichen Theiler haben, so folgt weiter

$$2. \quad [c; c+di][a+bi; c+di] = [ac+bd; c+di].$$

Ganz auf dieselbe Weise hat man

$$[a; a+bi][c+di; a+bi] = [ac+bd; a+bi],$$

folglich nach (§. 1.)

$$3. \quad [a; a-bi][c+di; a+bi]^3 = [ac+bd; a-bi].$$

Die Gleichungen (2.) und (3.), nach den bekannten Formeln in einander multiplicirt, geben

$$4. \quad [c; c+di][a; a-bi][a+bi; c+di][c+di; a+bi]^3$$
$$= [ac+bd; ac+bd+(ad-bc)i].$$

Um die vorkommenden Symbole für den gegenwärtigen Zweck und für die Anwendung der bereits bewiesenen Sätze passend einzurichten, mögen die

Buchstaben δ, ε, ζ alle drei ± 1 bedeuten, und zwar in der Weise, dafs

$$a \equiv \delta \pmod{4}, \quad c \equiv \varepsilon \pmod{4}, \quad ac+bd \equiv \zeta \pmod{4}$$

ist. Dann erhält man, da δa, εc, $\zeta(ac+bd)$ primär und reell sind,

$$[\delta a; a-bi] = [a-bi; a] = [-bi; a] = [i; a],$$

weil $a-bi \equiv -bi \pmod{a}$ und $-b$ reell ist. Eben so

$$[\varepsilon c; c+di] = [c+di; c] = [di; c] = [i; c],$$

$$[\zeta(ac+bd); ac+bd+i(ad-bc)] = [ac+bd+i(ad-bc); ac+bd]$$
$$= [i(ad-bc); ac+bd] = [i; ac+bd].$$

Durch Benutzung dieser Werthe läfst sich aus (4.) die folgende Gleichung ableiten:

$$5. \quad [i; ac][\zeta; ac+bd+i(ad-bc)][a+bi; c+di][c+di; a+bi]^3$$
$$= [\delta; a-bi][\varepsilon; c+di][i; ac+bd].$$

Aber b und d sind beide gerade, folglich ist $ac+bd \equiv ac \pmod{4}$ und $\zeta = \delta\varepsilon$. Dies giebt

$$[\zeta; ac+bd+i(ad-bc)] = [\delta; a-bi][\delta; c+di][\varepsilon; a-bi][\varepsilon; c+di],$$

und bemerkt man noch, dafs nach (§. 1.)

$$[\delta; c+di] = \delta^{\frac{1}{2}(c-1)} = (-1)^{\frac{1}{2}(a-1)\cdot\frac{1}{2}(c-1)}, \quad [\varepsilon; a-bi] = \varepsilon^{\frac{1}{2}(a-1)} = (-1)^{\frac{1}{2}(a-1)\cdot\frac{1}{2}(c-1)},$$

$$[i, ac] = \frac{1}{[i; ac]}, \quad [c+di; a+bi]^3 = \frac{1}{[c+di; a+bi]}$$

ist, so kann man der Gleichung (5.) die einfachere Form

$$6. \quad [a+bi; c+di] = [c+di; a+bi][i; ac(ac+bd)]$$

geben. Da nun $ac(ac+bd) = a^2c^2+abcd$, welche Zahl wir für einen Augenblick durch e bezeichnen wollen, $\equiv 1 \pmod{4}$, also primär ist, so hat man $[i; e] = i^{\frac{1}{2}(e-1)} = (-1)^{\frac{1}{4}(e-1)}$, also $= +1$ oder $= -1$, je nachdem $e \equiv 1$, oder $\equiv 5 \pmod{8}$ ist. Der erste Fall findet Statt, wenn die geraden Zahlen b und d entweder beide durch 4 theilbar sind, oder wenn wenigstens eine von ihnen es ist; und in diesem Falle hat man $[a+bi; c+di] = [c+di; a+bi]$. Ist aber sowohl b als auch $d \equiv 2 \pmod{4}$, so hat man $e \equiv 5 \pmod{8}$, also $[i, e] = -1$, und in diesem Falle ist aus (6.)

$$[a+bi; c+di] = -[c+di; a+bi].$$

Die beiden Fälle, welche wir eben betrachtet haben, lassen sich in der folgenden Formel vereinigen:

$$7. \quad [a+bi; c+di] = (-1)^{\frac{1}{2}(a-1)\cdot\frac{1}{2}(c-1)}[c+di; a+bi],$$

denn diese beiden Fälle lassen sich auch so characterisiren, dafs in dem einen die ungeraden Zahlen a und c beide, oder doch wenigstens eine von ihnen $\equiv 1 \pmod{4}$, dagegen in dem andern a und c beide $\equiv 3 \pmod{4}$ sind.

Um wieder auf die complexen Zahlen $A+bi$ und $C+di$ zurückzukommen, verbinden wir die Gleichungen (7.) mit den im Anfange dieses Paragraphs aufgestellten Gleichungen, welches

$$[A+Bi; C+Di] = (-1)^{\frac12(a-1)\cdot\frac12(c-1)}[C+Di; A+Bi]$$

giebt, oder auch, da m und $n \equiv 1 \pmod 4$, also $A \equiv a$ und $C \equiv c \pmod 4$ ist:

$$8. \quad [A+Bi; C+Di] = (-1)^{\frac12(A-1)\cdot\frac12(C-1)}[C+Di; A+Bi].$$

Diese Formel umfaſst alle Fälle und enthält das allgemeinste Reciprocitätsgesetz, welches sich in der Theorie der biquadratischen Reste aufstellen läſst.

„*Wenn* $A+Bi$ *und* $C+Di$ *irgend zwei ganze complexe Zahlen*
„$\equiv 1 \pmod{2+2i}$ *bezeichnen, so ist*

$$[A+Bi; C+Di] = [C+Di; A+Bi](-1)^{\frac12(A-1)\cdot\frac12(C-1)},$$

„*oder der biquadratische Character der ersten in Bezug auf die zweite*
„*ist identisch mit dem biquadratischen Character der zweiten in Bezug*
„*auf die erste, wenn entweder die eine und die andere, oder wenig-*
„*stens eine von ihnen* $\equiv 1 \pmod 4$ *ist; sind aber beide complexe*
„*Zahlen* $\equiv 3+2i \pmod 4$, *so unterscheiden sich jene beiden biqua-*
„*dratischen Charactere um zwei Einheiten.*"

Durch ganz ähnliche Betrachtungen, wie die hier angestellten, läſst sich auch das Reciprocitätsgesetz für die cubischen Reste beweisen.

§. 9.

Criterien für die complexe Zahl $1+i$.

Um für die Theorie der biquadratischen Reste nichts zu wünschen übrig zu lassen, wollen wir noch mit Hülfe derselben Principien, welche bisher in dieser Abhandlung angewandt wurden, die Criterien des biquadratischen Characters der complexen Zahl $1+i$ behandeln.

Betrachten wir zuerst den Fall, wenn der Modul reell ist. Es sei a eine reelle Primzahl $\equiv 1 \pmod 4$, und es sei der Werth von $[1+i; a]$ zu finden. Es sind zwei Fälle zu unterscheiden, je nachdem entweder $a = p = p_1 p_2$, wo p eine positive Primzahl $4n+1$ ist, oder $a = -q$ ist, wo q eine positive Primzahl $4n+3$ bedeutet. Im ersten Falle findet man

$$[1+i; p] = [1+i; p_1][1+i; p_2] = [1+i; p_1][1-i; p_1]^3$$
$$= [-4; p_1][i; p_1] = [i; p_1],$$

weil $-4 = (1+i)^4$, also ein Biquadrat ist. Aber $[i; p_1] = i^{\frac14(p-1)}$, also kommt für $a = p$:

$$[1+i; a] = i^{\frac14(a-1)}.$$

Im zweiten Falle, d. h. für $a = -q$, hat man

$$[1+i; -q] \equiv (1+i)^{\frac{1}{4}(q^2-1)} \pmod{q}.$$

Da nun wegen $q \equiv 3 \pmod{4}$ offenbar

$$(1+i)^q \equiv 1-i \pmod{q}, \text{ also}$$

$$(1+i)^{q-1} \equiv \frac{1-i}{1+i} \equiv -i \pmod{q}$$

ist, so erhält man

$$[1+i; -q] \equiv (1+i)^{(q-1)\cdot\frac{1}{4}(q+1)} \equiv (-i)^{\frac{1}{4}(q+1)} \pmod{q};$$

also kommt, eben wie im ersten Falle,

$$[1+i; a] = (-i)^{\frac{1}{4}(q+1)} = i^{\frac{1}{4}(a-1)}.$$

Es seien nun $a, a', a'', \ldots.$ reelle und primäre Primzahlen, gleich oder ungleich, in beliebiger Anzahl, als theils reelle Primzahlen $4n+1$ mit dem positiven, theils reelle Primzahlen $4n+3$ mit dem negativen Zeichen genommen, und es sei $aa'a'' \ldots. = A$. Setzt man

$$\tfrac{1}{4}(a-1) = \mu, \quad \tfrac{1}{4}(a'-1) = \mu', \quad \tfrac{1}{4}(a''-1) = \mu'', \quad \text{etc.},$$

so ist

$$a = 4\mu+1, \quad a' = 4\mu'+1, \quad a'' = 4\mu''+1, \text{ etc.}$$

Multiplicirt man alle diese Gleichungen in einander, so kommt

$$aa'a'' \ldots. = 1+4(\mu+\mu'+\mu''+\ldots.)+ \text{ einer Summe von Gliedern,}$$

die alle durch 16 theilbar sind. Hieraus folgt

$$\tfrac{1}{4}(aa'a'' \ldots. -1) \equiv \mu+\mu'+\mu''+\ldots. \pmod{4}, \text{ d. h.}$$

$$\tfrac{1}{4}(A-1) \equiv \tfrac{1}{4}(a-1)+\tfrac{1}{4}(a'-1)+\tfrac{1}{4}(a''-1)+\ldots. \pmod{4}.$$

Von der andern Seite hat man, dem oben Bewiesenen zufolge,

$$[1+i; a] = i^{\mu}, \quad [1+i; a'] = i^{\mu'}, \quad [1+i; a''] = i^{\mu''}, \quad \text{etc.};$$

folglich durch Multiplication, und mit Rücksicht auf die eben abgeleitete Congruenz:

$$[1+i; A] = i^{\mu+\mu'+\mu''+\ldots.} = i^{\frac{1}{4}(A-1)}.$$

Aber A stellt jede beliebige reelle primäre Zahl vor: mithin haben wir folgenden Satz über den biquadratischen Character der Zahl $1+i$ in Bezug auf reelle Zahlen:

„*Wenn A irgend eine reelle und primäre Zahl vorstellt, so ist der biquadratische Character von* $1+i$ *in Bezug auf A, gleich* $\frac{1}{4}(A-1)$."

Wir gehen zu der Vergleichung von $1+i$ mit einer *zweigliedrigen* primären Zahl $a+bi$ über und nehmen zuerst an, dafs a und b keinen gemeinschaftlichen Theiler haben. Ganz wie bei dem Übergange in §. 8. ergiebt sich mit Hülfe der bereits bewiesenen Sätze auch hier Alles aus der Betrachtung einer identischen Gleichung, nämlich der folgenden:

$$(\alpha.)\quad a(1+i)-(a+b) = i(a+bi)\ ^{*)}.$$

Diese Gleichung liefert die beiden folgenden Congruenzen:

$$(\beta.)\quad a(1+i) \equiv a+b\ (\text{mod. } a+bi),$$

$$(\gamma.)\quad a+bi \equiv -ai(1+i)\ (\text{mod. } a+b).$$

Die Congruenz (β.) giebt $[a;a+bi][1+i;a+bi] = [a+b;a+bi]$. Da $a+bi$ primär, folglich $a+b\equiv 1$ (mod. 4) ist, so folgt aus dem Lehrsatze §. 7. $[a+b;a+bi]=[a+bi;a+b]$, und die Congruenz (γ.) liefert wiederum $[a+bi;a+b] = [-ai;a+b][1+i;a+b]$, welches nach den Sätzen in §. 1. und nach dem vorhin bewiesenen Satze $= i^{\frac{3}{2}(a+b-1)}.i^{\frac{1}{4}(a+b-1)} = i^{\frac{3}{4}(a+b-1)}$ ist; also kommt, durch Einsetzung dieses Werthes:

$$(\delta.)\quad [a;a+bi][1+i;a+bi] = i^{\frac{3}{4}(a+b-1)}.$$

Ist nun zuerst $a+bi\equiv 1$ (mod. 4), also $a\equiv 1$, $b\equiv 0$ (mod. 4), so hat man nach dem Lehrsatze §. 7. und nach den Sätzen §. 1.

$$[a;a+bi] = [a+bi;a] = [bi;a][i;a] = i^{\frac{3}{2}(a-1)},$$

also geht (δ.) in

$$(\varepsilon.)\quad [1+i;a+bi] = i^{\frac{3}{4}(a+b-1)}.i^{-\frac{3}{2}(a-1)},$$

d. h., weil b durch 4 theilbar ist, in

$$(\text{I.})\quad [1+i;a+bi] = i^{\frac{1}{4}(a-b-1)},\qquad (a+bi \equiv 1\ (\text{mod. } 4))$$

über. Wenn aber $a+bi\equiv 3+2i$ (mod. 4) ist, also $a\equiv 3$, $b\equiv 2$ (mod. 4), so ist $-a\equiv 1$ (mod. 4), folglich $[a;a+bi]=[-1;a+bi][-a;a+bi]= -[a+bi;-a] = -[bi;-a] = -[i;-a] \equiv -i^{\frac{3}{2}(-a-1)}$. Substituirt man diesen Werth in der Gleichung (δ.), zieht die Exponenten von i zusammen und bemerkt dabei, dafs $b-2$ durch 4 theilbar ist, so erhält man

$$(\text{II.})\quad [1+i;a+bi] = i^{\frac{1}{4}(a-b-5)},\qquad (a+bi \equiv 3+2i\ (\text{mod. } 4)).$$

Diese beiden Resultate (I.) und (II.), welche sich leicht in den Ausdruck

$$(\text{III.})\quad [1+i;a+bi] = i^{\frac{1}{4}(a-b-b^2-1)}$$

vereinigen lassen, sind dieselben, welche *Gaufs* für Primzahlen in No. 63. seiner Untersuchungen über die biquadratischen Reste durch Induction gefunden und in den 9 letzten Nummern derselben Abhandlung auf einem von dem gegenwärtigen gänzlich verschiedenen Wege bewiesen hat.

Um zu dem allgemeinsten Falle überzugehen, sei $A+Bi=m(a+bi)$, m reell und $\equiv 1$ (mod. 4), $a+bi$ von derselben Form wie vorhin, nämlich

---

*) Es ist zu bemerken, dafs die vier Zahlen a, $1+i$, $a+b$, $a+bi$, zu je zweien genommen, keinen gemeinschaftlichen Theiler haben. Dies folgt unmittelbar daraus, dafs a ungerade ist, und dafs a als zu b relative Primzahl vorausgesetzt wird.

primär und a und b seien ohne gemeinschaftlichen Theiler. Dann hat man

$$[1+i;\,A+Bi] = [1+i;\,m][1+i;\,a+bi].$$

Aber dem bereits Bewiesenen zufolge ist

$$[1+i;\,m] = i^{\frac{1}{4}(m-1)},\quad [1+i;\,a+bi] = i^{\frac{1}{4}(a-b-b^2-1)}.$$

Da nun offenbar

$$\tfrac{1}{4}(m-1)+\tfrac{1}{4}(a-b-b^2-1) \equiv \tfrac{1}{4}(am-bm-b^2m^2-1) \pmod{4}$$

ist, so erhält man, analog mit der Formel (III.) und diese als speciellen Fall umfassend:

$$\text{(IV.)}\quad [1+i;\,A+Bi] = i^{\frac{1}{4}(A-B-B^2-1)},$$

für jede primäre complexe Zahl $A+Bi$.

„Für jede primäre complexe Zahl $A+Bi$, den Fall $B=0$ nicht ausgeschlossen, ist also der biquadratische Character von $1+i$ in Bezug auf $A+Bi$ gleich $\frac{1}{4}(A-B-B^2-1)$."

§. 10.

Algorithmus.

Da jede ganze complexe Zahl Q sich auf die Form

$$i^{\alpha}.(1+i)^{\beta}.P$$

bringen läfst, wo P primär ist, und man in jedem Symbol von der Form $[Q;\,R]$, unbeschadet der Allgemeinheit, R als primär voraussetzen darf, so lassen sich vermittels des Fundamentaltheorems und der Sätze über die complexen Zahlen i und $1+i$ alle Fragen über biquadratische Charactere lösen.

Mit Hülfe der vier Gleichungen

$$\text{(1.)}\quad [A+Bi;\,C+Di] = (-1)^{\frac{1}{4}(A-1).\frac{1}{4}(C-1)}[C+Di;\,A+Bi],$$

$$\text{(2.)}\quad [i;\,A+Bi] = i^{\frac{3}{4}(A-1)},$$

$$\text{(3.)}\quad [1+i;\,A+Bi] = i^{\frac{1}{4}(A-B-B^2-1)},$$

$$\text{(4.)}\quad [L;\,M] = [L';\,M],$$

in denen $A+Bi$, $C+Di$ als primär und $L\equiv L' \pmod{M}$ vorausgesetzt werden, läfst sich ein einfacher Algorithmus angeben, vermittels dessen man den biquadratischen Character für je zwei vorgelegte complexe Zahlen in Bezug auf einander bestimmen kann. Nennen wir in dem Symbole $[Q;\,R]$ die Zahlen Q und R die *Elemente,* und denjenigen Factor, welcher herausgesetzt werden mufs (wie z. B. in (1.) $(-1)^{\frac{1}{4}(A-1).\frac{1}{4}(C-1)}$), damit man die Elemente mit einander vertauschen oder das Symbol *umkehren* könne, den *Modularfactor,* so besteht dieser Algorithmus, mit zwei Worten characterisirt, in einem fortwährenden Umkehren, Heraussetzen des Modularfactors und Bestimmung des klein-

sten Restes des ersten Elements in Bezug auf das zweite als Divisor; immer mit Anwendung der Gleichungen (1.) bis (4.), bis man zu den kleinsten complexen Zahlen gelangt.

Es seien P und P_1 zwei gegebene *primäre* complexe Zahlen, und es sei der Werth von $[P, P_1]$ zu finden: denn auf diesen Fall lassen sich alle übrigen sogleich vermittels (2.) und (3.) zurückführen. Man bilde ein Divisionsschema von der Form

$$(\varphi.)\qquad \begin{aligned} P &= k_1 P_1 + \varepsilon_1 P_2, \\ P_1 &= k_2 P_2 + \varepsilon_2 P_3, \\ P_2 &= k_3 P_3 + \varepsilon_3 P_4, \\ &\ldots\ldots\ldots \\ P_{\mu-2} &= k_{\mu-1} P_{\mu-1} + \varepsilon_{\mu-1} P_\mu, \\ P_{\mu-1} &= k_\mu P_\mu, \end{aligned}\qquad (\varphi.)$$

wo P, P_1, P_2, P_3 etc. lauter *primäre* complexe Zahlen vorstellen; $\varepsilon_1, \varepsilon_2, \varepsilon_3$ etc. sind sämmtlich von der Form $i^\alpha(1+i)^\beta$, während $\varepsilon_1 P_2$, $\varepsilon_2 P_3$, $\varepsilon_3 P_4$, etc. die absolut kleinsten Reste sind von resp. P in Beziehung auf den Divisor P_1, P_1 in Beziehung auf den Divisor P_2, P_2 in Beziehung auf den Divisor P_3, u. s. w. Man findet den absolut kleinsten Rest, z. B. von P in Bezug auf den Divisor P_1, wenn man für den Quotienten $\frac{P}{P_1}$ die ganze complexe Zahl k_1 so bestimmt, dafs in der Differenz $\frac{P}{P_1} - k_1$ der reelle Theil, so wie der Coëfficient von i, $\leqq \frac{1}{2}$ ist und dann $\varepsilon_1 P_2 = P - k_1 P_1$ setzt. Diese Operation wird in dem Schema (φ.) nothwendig zu einer letzten Gleichung $P_{\mu-1} = k_\mu P_\mu$ führen, in welcher der Rest $=0$ ist: denn die Norm jedes Restes ist nicht gröfser als die halbe Norm des vorhergehenden Divisors, so dafs die Normen der Reste eine stark abnehmende Reihe bilden, deren Endglied die Null sein mufs. Nun ist entweder $P_\mu = 1$, oder nicht $= 1$. Im zweiten Fall haben P und P_1 einen gemeinschaftlichen Factor und man erhält $[P; P_1] = 0$. Im ersten Falle hat man zur Bestimmung von $[P; P_1]$ folgende Reihe von Gleichungen:

$$\begin{aligned} [P; P_1] &= [\varepsilon_1 P_2; P_1] = [\varepsilon_1; P_1][P_1; P_2]\mathfrak{M}(P_1, P_2), \\ [P_1; P_2] &= [\varepsilon_2 P_3; P_2] = [\varepsilon_2; P_2][P_2; P_3]\mathfrak{M}(P_2, P_3), \\ [P_2; P_3] &= [\varepsilon_3 P_4; P_3] = [\varepsilon_3; P_3][P_3; P_4]\mathfrak{M}(P_3, P_4), \\ &\ldots\ldots\ldots\ldots\ldots \\ [P_{\mu-2}; P_{\mu-1}] &= [\varepsilon_{\mu-1}; P_{\mu-1}]; \end{aligned}$$

wo allgemein durch $\mathfrak{M}(A+Bi, C+Di)$ der Modularfactor $(-1)^{\frac{1}{4}(A-1)\cdot\frac{1}{4}(C-1)}$

bezeichnet wird; und hieraus ergiebt sich

$$[P; P_1] = [\varepsilon_1, P_1][\varepsilon_2; P_2][\varepsilon_3; P_3] \ldots\ldots [\varepsilon_{\mu-1}, P_{\mu-1}]$$
$$\times \mathfrak{M}(P_1, P_2)\mathfrak{M}(P_2, P_3)\mathfrak{M}(P_3, P_4) \ldots\ldots \mathfrak{M}(P_{\mu-2}, P_{\mu-1}).$$

Die Werthe von $[\varepsilon_1; P_1]$, $[\varepsilon_2; P_2]$ u. s. w. ergeben sich unmittelbar aus den Gleichungen (2.) und (3.), während man zur Bestimmung des Productes der Modularfactoren $\mathfrak{M}$ nur zu zählen braucht, für wie viele von ihnen zwei *aufeinanderfolgende* P beide zugleich $\equiv 3+2i$ (mod. 4) sind. So erhält man den Werth von $[P; P_1]$ durch den bloßen Anblick der complexen Zahlen P, P_1, P_2, P_3, etc. Durch die Bildung eines Divisionsschemas (φ.), welches in den andern Theilen der Zahlentheorie so wesentliche Dienste leistet, indem es die Verwandlung eines gewöhnlichen Bruchs in einen Kettenbruch, den größten gemeinschaftlichen Theiler zweier Zahlen, die Auflösung der Congruenzen ersten Grades giebt, kann also auch der biquadratische Character jeder complexen Zahl auf die einfachste Weise bestimmt werden. Durch diesen einfachen Algorithmus wird gewissermaßen der Theorie der biquadratischen Reste die letzte Vollendung gegeben.

Es ist fast überflüssig, zu bemerken, daß durch die Theorie der biquadratischen Reste auch die der quadratischen Reste für die complexen Zahlen vollständig absolvirt ist.

20.

Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste.

(Von Herrn Stud. *Gotth. Eisenstein* zu Berlin.)

Es sei p eine positive ungerade Primzahl, a der Complexus aller *geraden* Zahlen $<p$ und >0, also $a=2, 4, \ldots. 6, p-1$; q sei irgend eine durch den Modul p nicht theilbare ganze Zahl. Bezeichnet man durch r das allgemeine Glied der Reste der Vielfachen qa nach dem mod. p, so werden offenbar die Zahlen der Reihe, deren allgemeines Glied $(-1)^r . r$ ist, mit den Zahlen der Reihe a bis auf Vielfache von p übereinstimmen; also wird man die beiden Congruenzen haben:

$$q^{\frac{1}{2}(p-1)}\Pi a \equiv \Pi r \text{ (mod. } p), \quad \text{und} \quad \Pi a \equiv (-1)^{\Sigma r}\Pi r \text{ (mod. } p),$$

woraus folgt

$$q^{\frac{1}{2}(p-1)} \equiv (-1)^{\Sigma r} \text{ (mod. } p), \quad \text{also} \quad \left(\frac{q}{p}\right) = (-1)^{\Sigma r}.$$

Bedeutet $E\left(\frac{qa}{p}\right)$ die gröſste in dem Bruche $\frac{qa}{p}$ steckende ganze Zahl, so ist offenbar $\Sigma qa = p\Sigma E\left(\frac{qa}{p}\right) + \Sigma r$; und da alle a *gerade* sind, und $p\equiv 1$ (mod. 2) ist, so folgt hieraus $\Sigma r \equiv \Sigma E\left(\frac{qa}{p}\right)$ (mod. 2); also ist auch

$$\left(\frac{q}{p}\right) = (-1)^{\Sigma E\left(\frac{qa}{p}\right)}$$

Wenn $q=2$ ist, so giebt diese Formel sogleich den Werth von $\left(\frac{2}{p}\right)$: ist dagegen q ungerade, also $q-1$ gerade, so findet man durch eine leichte Transformation

$$\Sigma E\left(\frac{qa}{p}\right) \equiv -E\left(\frac{a}{p}\right) + E\left(\frac{2a}{p}\right) - E\left(\frac{3a}{p}\right) + \ldots. \pm E\left(\frac{\frac{1}{2}(q-1)a}{p}\right)$$

$$\equiv \quad E\left(\frac{a}{p}\right) + E\left(\frac{2a}{p}\right) + E\left(\frac{3a}{p}\right) + \ldots. + E\left(\frac{\frac{1}{2}(q-1)a}{p}\right) \text{ (mod. 2)}.$$

Wird letztere Summe durch μ bezeichnet, so hat man auch $\left(\frac{q}{p}\right) = (-1)^{\mu}$.

Man stelle sich jetzt in der Ebene ein rechtwinkliges Coordinatensystem (x, y) und die ganze Ebene durch Parallelen mit den Axen in den Abständen $=1$ von einander in lauter Quadrate von den Dimensionen $=1$ getheilt vor.

Gitterpuncte sollen alle Eckpuncte von Quadraten heifsen, welche nicht in den beiden Coordinaten-Axen liegen (Taf. II. Fig. 1. 2.).

Nimmt man auf irgend einer senkrechten Parallele einen Punct an, dem die Ordinate y entspricht, so wird $E(y)$ die Anzahl der Gitterpuncte ausdrücken, welche zwischen diesem Puncte und der wagerechten Axe liegen; und nimmt man auf irgend einer wagerechten Parallele einen Punct an, dem die Abscisse x entspricht, so wird $E(x)$ die Anzahl der Gitterpuncte ausdrücken, welche zwischen diesem Puncte und der senkrechten Axe liegen. Zeichnet man daher in der Ebene irgend eine Curve, deren Gleichung $y=\varphi(x)$ ist (Fig. 1.), so wird die Summe

$$E\varphi(1)+E\varphi(2)+E\varphi(3)+E\varphi(4)+\text{ etc.}$$

die Anzahl der Gitterpuncte geben, welche zwischen dieser Curve und der Axe der x liegen, diejenigen Gitterpuncte mitgerechnet, welche etwa zufällig auf der Curve selbst liegen sollten.

Es sei nun, um wieder auf unsern Gegenstand zu kommen, AB (Fig. 2.) diejenige gerade Linie, deren Gleichung $y=\frac{q}{p}x$ ist, wo p und q jetzt beide als positive ungerade *Primzahlen* vorausgesetzt werden. $AD=FB$ sei $=p$, $AF=DB=q$, $AC=EG=\frac{1}{2}(p-1)$, $AE=CG=\frac{1}{2}(q-1)$. Bezeichnet man durch μ die Anzahl der Gitterpuncte zwischen AB und AD, bis zur Ordinate CG incl. (welche in der Figur durch Sternchen (*) ausgezeichnet sind), so wird man nach dem oben Bewiesenen $\left(\frac{q}{p}\right)=(-1)^{\mu}$ haben. Da die Gleichung unserer Geraden auch so geschrieben werden kann: $x=\frac{p}{q}y$, so wird man auf dieselbe Weise, wenn ν die Anzahl der Gitterpuncte bezeichnet, welche zwischen AB und AF bis zur Abscisse EG incl. liegen (welche durch kleine Nullen (°) ausgezeichnet sind), $\left(\frac{p}{q}\right)=(-1)^{\nu}$ haben. Offenbar erschöpfen aber alle mit * und alle mit ° bezeichneten Gitterpuncte zusammengenommen, d. h. alle Gitterpuncte *rechts* und alle Gitterpuncte *links* von AB, *sämmtliche* Gitterpuncte des Rechtecks $AEGC$, deren Anzahl $\frac{1}{2}(p-1).\frac{1}{2}(q-1)$ ist; also ergiebt sich $\mu+\nu=\frac{1}{2}(p-1).\frac{1}{2}(q-1)$, und

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\mu+\nu}=(-1)^{\frac{1}{2}(p-1).\frac{1}{2}(q-1)};$$

was zu beweisen war.

Übrigens läfst sich die obige Transformation $\Sigma E\left(\frac{qa}{p}\right) \equiv \mu \pmod{2}$ ebenfalls durch eine sehr einfache geometrische Betrachtung nachweisen, wenn man bedenkt, dafs $\Sigma E\left(\frac{qa}{p}\right)$ nichts anders ist, als die Anzahl der Gitterpuncte, welche auf den *geraden* Ordinaten (denen die Abscissen $x = 2, 4, 6, \ldots p-1$ entsprechen) zwischen AB und AD bis zu BD liegen, und dafs jede Ordinate, von der Axe AD bis zu FB excl. hin, $q-1$, also eine gerade Anzahl Gitterpuncte enthält; so wie, dafs die beiden Dreiecke BAD und ABF congruent sind und dafs dieses in Bezug auf BF und BD genau ebenso liegt, wie jenes in Bezug auf AD und AF; wovon die Ausführung dem Leser überlassen bleiben mag.

Anmerkung. Es giebt Figuren, für welche man durch einfache Formeln die Anzahl der innerhalb derselben liegenden Gitterpuncte bestimmen kann. Stellt man sich z. B. einen Kreis vor, dessen Mittelpunct im Anfangspuncte der Coordinaten liegt und dessen Radius $= \sqrt{m}$ ist, so wird die Anzahl der Gitterpuncte S, welche dieser Kreis umschliefst, die auf den Axen liegenden mitgerechnet, durch folgende Formel gegeben:

$$S = 1 + 4(E(m) - E(\tfrac{1}{3}m) + E(\tfrac{1}{5}m) - E(\tfrac{1}{7}m) + \ldots),$$

bis die Reihe von selbst abbricht. Wie leicht zu sehen, drückt diese Gleichung eine Relation zwischen der Anzahl der Gitterpuncte eines *Kreises* und der Anzahl der Gitterpuncte eines zwischen zwei *Hyperbeln* eingeschlossenen Segments aus. Setzt man in der Formel

$$\frac{1}{m}S = \frac{1}{m} + 4\left(\frac{1}{m}E(m) - \frac{1}{m}E(\tfrac{1}{3}m) + \frac{1}{m}E(\tfrac{1}{5}m) - \text{ etc.}\right),$$

$m = \infty$, so verwandelt sich die linke Seite in π, während die rechte Seite in $4(1 - \frac{1}{3} + \frac{1}{5} - \text{ etc.})$ übergeht, so dafs man hier die *Leibnitz*'sche Formel für π erhält. Es giebt ähnliche Formeln für die Anzahl der Gitterpuncte eines Systems von Ellipsen oder Hyperbelsectoren; auch finden ähnliche Relationen im Raume und in Fällen mit mehr als 3 Dimensionen Statt. Wir werden auf diesen wichtigen Gegenstand, der aufs genauste mit den Eigenschaften der höheren Formen zusammenhängt, bei einer andern Gelegenheit zurückkommen.

Berlin, im Juli 1844.

21.

Exercitationes analyticae in theoremate Abelianum de integralibus functionum algebraicarum.

(Auctore Dr. *Georgio Rosenhain* Breslav.)

Si per $f(x, y)$ designamus functionem rationalem variabilis x et radicis cuiuslibet y aequationis algebraicae

$$1.\quad \varphi(x,y) = p_0 y^n + p_1 y^{n-1} + p_2 y^{n-2} + \ldots + p_{n-1} y + p_n = 0,$$

cuius coëfficientes $p_0, p_1, p_2, \ldots p_n$ polynomia data ipsius x sunt, functioni $f(x, y)$ nomen tribuitur algebraicae ipsius x, eique explicitae aut implicitae, prout aequatio (1.) per radicum extractionem resolvi potest aut non potest. Inter varias formas, in quas aequationis (1.) et formularum, quibus radicum functiones symmetricae ad coëfficientes revocantur, notissimarum ope functionem $f(x, y)$ redigere licet, eam geometrae plerumque eligunt, quae, denominatore rationali facto, respectu ipsius y evadit integra; scilicet formam

$$2.\quad M_1 y^{n-1} + M_2 y^{n-2} + M_3 y^{n-3} + \ldots + M_{n-1} y + M_n,$$

in qua coëfficientes $M_1, M_2, M_3, \ldots M_n$ sunt functiones rationales ipsius x. Sed casus inveniuntur, quibus peculiari denominatoris forma irrationali vera functionis algebraicae indoles continetur, quae, denominatore rationali facto, certe in functione algebraica implicita valde obumbratur. In quorum numero inprimis sunt differentialia tota functionis $f(x, y)$, quae ex ipsa differentiatione differentialis partialis functionis $\varphi(x, y)$ secundum y sumti (quod more *Lagrangiano* signo $\varphi'(y)$ designare placet) potestates impares ex ordine denominatores asciscunt. Eodem modo, ubi de ***integralibus*** functionum algebraicarum agitur, functioni integrandae, siquidem eius formam accuratius definire volumus, haud inconvenienter suppeditabimus denominatorem $\varphi'(y)$, unde respecto y functio ista formam induet primi quotientis differentialis functionis algebraicae (2.) ipsius x. Facta autem divisione per denominatorem $\varphi'(y)$, numerator functionis integrandae repectu ipsius y ad gradum $(n-2)^{\text{tum}}$ deprimitur, ita ut, si $Q_2, Q_3, \ldots Q_n$ functiones rationales ipsius x significant,

$$3.\quad \frac{Q_2 y^{n-2} + Q_3 y^{n-3} + \ldots + Q_{n-1} y + Q_n}{\varphi'(y)}$$

sit forma functionis algebraicae integrandae, quam inter omnes praestantissimam esse censemus. Quia enim, respecto y, eadem est ac forma primi quotientis

differentialis functionis algebraicae (2.), simplicius quam quaevis alia docebit, quae relationes inter coëfficientes constantes functionis algebraicae integrandae intercedere debeant, ut eius integrale algebraice exhiberi possit, sive ut functio integranda sit differentiale totum functionis algebraicae ipsius x. Quae quidem quaestio, ubi de istis integralibus agitur, et sponte occurrit, (nam inter casus algebraicos et transcendentes distinguendum esse, ab initio patet) et simul aliam expedit de eorum reductione algebraica, sive de integralibus, ad quorum aggregatum lineare addita functione algebraica ipsius x omnia alia integralia functionum algebraicarum eiusdem irrationalitatis revocantur. Quantum autem et in disquisitionibus de additione integralium functionum algebraicarum forma (3.) functionis integrandae ante alias excellat, in ipsa commentatione apparebit.

Posito $n=2$ forma (3.) in eam abit, cui, in integralibus circularibus et ellipticis semper adhibitae, clarissimus *Abel* inclytum superstruxit de integralibus hyperellipticis theorema; quod etiam ex aequatione quadratica *trinomia* deducere, clarissimo *Jacobi* (vide Diar. Crell. tom. X. pag. 99) nonnisi ope eiusdem formae (3.) successit. In nota brevissima (Diar. Crell. tom. IV.), qua theorema suum ad integralia omnia functionum algebraicarum (vel implicitarum) extendit, clarissimus *Abel* non quaesivit de functionis integrandae forma aptissima, quia in brevissima demonstrationis expositione, quae spatio una pagina minore continetur, suffecit definitio generalis, ut functionis rationalis ipsarum x et radicis y aequationis n^{ti} gradus $\varphi(x, y) = 0$. Quominus, quod promiserat, rem uberius tractaret, mortem, quae paucas hebdomades postea eum abripuit, prohibuisse, notum est. Sic novum inventum geometris superstitibus perficiendum relictum erat. Sed rei gravissimae diu rationem non habuerunt. Triennio vero post clarissimus *Jacobi*, quum in Diario Crelliano (tom. VIII.) iudicaret de supplemento tertio operis egregii clarissimi *Legendre* „Traité des fonctions elliptiques," theorema inclytum *Abelianum* ex hyperellipticis ad cuiuslibet functionis algebraicae integralia ab ipso auctore extensum esse, geometris in memoriam reduxit, cuius tamen expositionem totam reproducendam esse censuit. Multi ex hoc tempore rem tractarunt. Sed non nisi eo casu, quo y per aequationem binomiam ex ipsa x pendet, ideoque $f(x, y)$ ipsius x est functio explicita, ex invento clarissimi *Abel* iis, quae ipse de integralibus hyperellipticis collegit, similia concludere potuerunt. Huc maxime pertinent integralium divisio in genera secundum naturam diversam, quam in additione prae se ferunt, atquae aequalitas numeri constantium, quae in numeratore integralis primi generis inveniuntur, cum numero minimo integralium, ad quem summa data integralium theoremate *Abeliano*

revocatur. Eadem etiam pro casu maxime generali aequationis (1.) valere, sequentibus astendere nobis proposuimus, atque apparebit demonstrationem maxime iuvari, ubi loco formae (2.) hucusque acceptae ipsa (3.) functioni integrandae tribuatur. Antea vero ostendamus, quomodo differentiale totum functionis algebraicae $f(x,y)$ ipsius x calculo minimo in formam (3.) redigatur; quo facto simul expedietur quaestio de reductione algebraica integralium functionum algebraicarum formae (3.).

Caput I.

De quotiente differentiali functionis algebraicae unius variabilis.

1.

Signis *Lagrangianis* usi significabimus per $f'(x)$ et $f'(y)$ differentialia partialia functionis $f(x,y)$ variabilium x et y secundum x et y sumta; atque, ubi y functio ipsius x est, per f' vel etiam per $[f(x,y)]'$ differentiale totum functionis $f(x,y)$, cuius in locum, ubi placuerit etiam signum *Leibnitzianum* $\frac{df(x,y)}{dx}$ scribetur.

Sit y radix quaelibet aequationis

$$1.\quad \varphi(x,y) = p_0 y^n + p_1 y^{n-1} + p_2 y^{n-2} + \dots + p_{n-1} y + p_n = 0,$$

in qua $p_0, p_1, p_2, \dots p_n$ sint polynomia data ipsius x ita comparata, ut aequatio (1.) irreductibilis sit, i. e. ut radix y aequationis (1.) non simul sit radix alterius aequationis rationalis inter x et y, quae respecto y tantum ad gradum n^{to} minorem ascendat; quo statuto aequatio (1.) radicibus aequalibus gaudere non poterit. Jam quia ex aequatione identica $\varphi(x,y) = 0$ differentiando prodit

$$\varphi'(x) + y'\varphi'(y) = 0 \quad \text{ideoque} \quad \frac{dy}{dx} = y' = -\frac{\varphi'(x)}{\varphi'(y)},$$

si per M_k functio rationalis ipsius x per k quilibet e numeris $1, 2, 3, \dots, n-1$ designatur, $\frac{d(M_k y^{n-k})}{dx}$ denominatore $\varphi'(y)$ gaudebit, et posito

$$\frac{d(M_k y^{n-k})}{dx} = \frac{F_k(y)}{\varphi'(y)}$$

erit

$$F_k(y) = (M_k y^{n-k})'\varphi'(y) = M'_k y^{n-k}\varphi'(y) - (n-k)M_k y^{n-k-1}\varphi'(x).$$

Numeratorem $F_k(y)$ videmus respectu ipsius y ascendere usque ad gradum $(2n-k-1)^{\text{tum}}$; ut ad $(n-1)^{\text{tum}}$ deprimatur, ponamus

$$F_k(u) = T_k(u)\varphi(x,u) + P_{1,k}u^{n-1} + P_{2,k}u^{n-2} + \dots + P_{n-1,k}y + P_{n,k},$$

ubi u significat quantitatem quamlibet, $T_k(u)$ autem functionem rationalem in-

tegram ipsius u gradus $(n-k-1)^{ti}$, cuius coëfficientes aeque ac quantitates $P_{m,k}$ functiones rationales ipsius x sunt; erit, quia $\varphi(x,y)=0$,

$$F_k(y) = P_{1,k}y^{n-1}+P_{2,k}y^{n-2}+\dots+P_{n-1,k}y+P_{n,k} = (M_k y^{n-k})'\varphi'(y),$$

et posito

$$4.\quad \varphi(x,u)=p_0u^n+p_1u^{n-1}+\dots+p_n=p_0(u-y_1)(u-y_2)(u-y_3)\dots(u-y_n),$$

e formula notissima de discerptione in fractiones simplices

$$5.\quad \frac{P_{1,k}u^{n-1}+P_{2,k}u^{n-2}+\dots+P_{n,k}}{\varphi(x,u)}$$

$$=\sum_1^n{}_i\frac{F_k(y_i)}{\varphi'(y_i)}\cdot\frac{1}{u-y_i}=\sum_1^n{}_i\frac{F_k(y_i)}{\varphi'(y_i)}\cdot\left\{\frac{1}{u}+\frac{y_i}{u_2}+\frac{y_i^2}{u_3}+\dots\right\}$$

multiplicatione facta per $\varphi(x,u)$ et valore $F_k(y_i)=(M_k y_i^{n-k})'\varphi'(y_i)$ substituto,

$$6.\quad P_{r+1,k}=\sum_1^n{}_i(p_0y_i^r+p_1y_i^{r-1}+p_2y_i^{r-2}+\dots+p_{r-1}y_i+p_r)(M_ky_i^{n-k})'.$$

Pars dextra aequationis (6.) est functio symmetrica radicum $y_1, y_2, \dots, y_n$ aequationis $\varphi(x,y)=0$, ideoque functio rationalis polynomiorum $p_0, p_1, p_2, \dots, p_n$ et ipsius M_k eorumque quotientium differentialium $p_0', p_1', p_2', \dots p_n'$, M_k', unde aequatione (6.) $P_{r+1,k}$ exhibetur ut functio rationalis ipsius x. Quibus collectis habemus aequationem

$$7.\quad \frac{d(M_ky^{n-k})}{dx}=\frac{P_{1,k}y^{n-1}+P_{2,k}y^{n-2}+P_{3,k}y^{n-3}+\dots+P_{n,k}}{\varphi'(y)},$$

in qua valores coëfficientium $P_{1,k}, P_{2,k}, \dots, P_{n,k}$ e formula (6.) inveniuntur ponendo $0, 1, 2, \dots, n-1$ loco ipsius r.

Pro $r=0$ invenitur e formula (6.)

$$8.\quad P_{1,k}=\sum_1^n{}_ip_0(M_ky_i^{n-k})'=p_0(M_k\sum_1^n{}_iy^{n-k})',$$

unde divisione facta per denominatorem $\varphi'(y)$ et quotiente divisionis $\frac{P_{1,k}}{np_0}$ ab utraque parte subducto aequatio (7.) abit in hanc:

$$9.\quad \frac{d\left\{M_k\left(y^{n-k}-\frac{1}{n}\sum_1^n{}_iy_i^{n-k}\right)\right\}}{dx}=\frac{Q_{2,k}y^{n-2}+Q_{3,k}y^{n-3}+\dots+Q_{n-1,k}y+Q_{n,k}}{\varphi'(y)},$$

in qua

$$10.\quad Q_{r+1,k}=P_{r+1,k}-\frac{n-r}{n}\cdot\frac{p_r}{p_0}P_{1,k}$$

$$=\sum_1^n{}_i\left\{(p_0y_i^r+p_1y_i^{r-1}+\dots+p_r)(M_ky_i^{n-k})'-\frac{n-r}{n}p_r(M_ky_i^{n-k})'\right\}$$

Posito igitur $\sum_1^{n-1}{}_kQ_{r+1,k}=N_{r+1}$ habemus formulam

$$11.\quad \frac{d\sum_1^{n-1}{}_k M_k\left(y^{n-k}-\frac{1}{n}\sum_1^n{}_i y_i^{n-k}\right)}{dx} = \frac{N_2 y^{n-2}+N_3 y^{n-3}+\dots+N_{n-1}y+N_n}{\varphi'(y)}$$

quae docet, ponendum esse

$$12.\quad -nM_n = \sum_1^n{}_i(M_1 y_i^{n-1}+M_2 y_i^{n-2}+\dots+M_{n-1}y_i),$$

ut, si y designat quamlibet e n radicibus $y_1, y_2, y_3, \dots, y_n$ aequationis n^{ti} gradus $\varphi(x,y)=0$, in differentiali functionis algebraicae ipsius x

$$M_1 y^{n-1}+M_2 y^{n-2}+\dots+M_{n-1}y+M_n$$

numerator respecto y sponte descendat ad gradum $(n-2)^{tum}$ unitate minorem quam gradus denominatoris $\varphi'(y)$, sive ut fiat

$$\frac{d(M_1 y^{n-1}+M_2 y^{n-2}+\dots+M_{n-1}y+M_n)}{dx} = \frac{N_2 y^{n-2}+N_3 y^{n-3}+\dots+N_{n-1}y+N_n}{\varphi'(y)}.$$

Qui valor ipsius M_n etiam directius hoc modo invenitur:

Quaesita functione M_n ipsius x eiusmodi, ut, quoties y sit una e radicibus $y_1, y_2, y_3, \dots, y_n$ aequationis $\varphi(x,y)=0$, fiat

$$\frac{d(M_1 y^{n-1}+M_2 y^{n-2}+\dots+M_{n-1}y+M_n)}{dx} = \frac{N_2 y^{n-2}+N_3 y^{n-3}+\dots+N_{n-1}y+N_n}{\varphi'(y)},$$

et $M_1, M_2, \dots, M_{n-1}, N_2, N_3, \dots, N_n$ sint functiones rationales solius x, ab ipsa y nullo modo pendentes, sequitur e theoremate notissimo

$$\sum_1^n{}_i \frac{N_2 y_i^{n-2}+N_3 y_i^{n-3}+\dots+N_{n-1}y_i+N_n}{\varphi'(y_i)} = 0,$$

$$\frac{d(M_1 \sum_1^n{}_i y_i^{n-1}+M_2 \sum_1^n{}_i y_i^{n-2}+\dots+M_{n-1}\sum_1^n{}_i y_i+nM_n}{dx} = 0,$$

unde $-nM_n$ valorem sibi poscit aequationis (12.).

2.

Accuratius examinemus coëfficientes $N_{r+1}=\sum_1^{n-1}{}_k Q_{r+1,k}$ singulis indicis r valoribus 1, 2, 3, ..., $n-1$ respondentes, et quaeramus de forma functionum M_k eiusmodi, ut ea potestas ipsius p_0, quam e proprietate notissima functionum symmetricarum radicum aequationis algebraicae $\varphi(x,y)=0$, functio N_{r+1} pro denominatore assumit, eius numeratorem metiatur. Quam quidem quaestionem casibus hucusque consideratis aequationis quadraticae trinomiae et aequationis binomiae n^{ti} gradus cuiuslibet eandem esse observo cum altera quaestione de minimo numero integro positivo λ eiusmodi, ut, posito $M_k = A_k p_0^{\lambda}$, in denominatoribus ipsarum $Q_{r+1,k}$, quibus functiones N_{r+1} conflantur, potesta-

tes illae ipsius p_0 non amplius inveniantur. Pro $n=2$ enim numeri r et k solum ipsius r valorem permittunt, unde numeri coëfficientium N_{r+1} et coëfficientium $Q_{r+1,k}$ uterque unitati aequales fiunt; casu vero aequationis binomiae, quo $p_1=p_2=p_3=\dots=p_{n-1}=0$, e coëfficientibus $Q_{r+1,k}$ eidem r respondentibus, omnes evanescunt praeter solam $Q_{r+1,r}$, unde fit $N_{r+1}=Q_{r+1,r}$. Qua de re etiam nostro casu aequationis generalis algebraicae n^{ti} gradus $\varphi(x,y)=0$, quamvis altera ab altera divergat, quaestioni illi de functionibus N_{r+1} brevem alterius quaestionis de ipsis $Q_{r+1,k}$ expositionem praemittere placet. Et primum patet ponendum esse $M_k=A_k p_0^\lambda$ ut potestas illa ipsius p_0 e denominatore functionis $Q_{r+1,k}$ exterminetur; atque erit valor minimus ipsius λ aequalis numero $n-k$, siquidem aequationis $\varphi(x,y)=0$ forma maxime generalis conservatur.

Eodem enim modo, quo ex aequatione

$$13.\quad \frac{\varphi'(u)}{\varphi(x,u)}=\sum_1^n{}_i\frac{1}{u-y_i}=\sum_1^n{}_i\left\{\frac{1}{u}+\frac{y_i}{u^2}+\frac{y_i^2}{u^3}+\frac{y_i^3}{u^4}+\dots\right\}$$

inveniuntur formulae

$$14.\quad \begin{cases} 1)\ 0=p_0\sum_1^n{}_i y_i^a+p_1\sum_1^n{}_i y_i^{a-1}+p_2\sum_1^n{}_i y_i^{a-2}+\dots+p_{a-1}\sum_1^n{}_i y_i+p_a.a, & \text{si } a\leqq n \text{ et} \\ 2)\ 0=p_0\sum_1^n{}_i y_i^a+p_1\sum_1^n{}_i y_i^{a-1}+p_2\sum_1^n{}_i y_i^{a-2}+\dots+p_n\sum_1^n{}_i y_i^{a-n}, & \text{si } a\geqq n, \end{cases}$$

legem continentes notissimam, qua superiorum potestatum radicum summae ad inferiorum revocantur, ex aequatione simili

$$15.\quad \frac{\varphi'(x)}{\varphi(x,u)}=\frac{p_0'}{p_0}-\sum_1^n{}_i\frac{y_i'}{u-y_i}=\frac{p_0'}{p_0}-\sum_1^n{}_i\frac{y_i'}{u}\left\{1+\frac{y_i}{u}+\frac{y_i^2}{u^2}+\frac{y_i^3}{u^3}+\dots\right\},$$

in qua loco ipsius $\frac{\varphi'(x)}{\varphi'(y_i)}$ eius valor $-y_i'$ substitutus est, proveniunt

$$16.\quad \begin{cases} 1)\ 0=p_0\sum_1^n{}_i y_i^{a-1}y_i'+p_1\sum_1^n{}_i y_i^{a-2}y_i'+\dots+p_{a-1}\sum_1^n{}_i y_i'+p_a\left\{\log\frac{p_a}{p_0}\right\}', & \text{si } a\leqq n \text{ et} \\ 2)\ 0=p_0\sum_1^n{}_i y_i^{a-1}y_i'+p_1\sum_1^n{}_i y_i^{a-2}y_i'+\dots+p_n\sum_1^n{}_i y_i^{a-n-1}y_i', & \text{si } a\geqq n. \end{cases}$$

Quarum aequationum ope, vel etiam si vis ope similium, quae, aequatione (14. 1.) ab ipsa $\sum_1^n{}_i y^{-n+a}\varphi(x,y_i)=0$ et aequatione (16. 1.) ab ipsa $\sum_1^n{}_i y_i^{-n+a-1}y_i'\varphi(x,y_i)=0$ subductis, pro summis potestatum negativarum radicum obtinentur, valor functionis $Q_{r+1,k}$ aequatione (10.) exhibitus ita transformatur, ut positis

$$17.\quad M_k=A_k p_0^{n-k},\quad p_0^r\sum_1^n{}_i y_i^r=S_r,\quad Q_{r+1,k}=A_k'B_{r,k}+(n-k)A_kT_{r,k}$$

fiat, si $r\leqq k$:

$$18. \begin{cases} 1) & -R_{r,k} = \frac{n-r}{n} p_r S_{n-k} + p_0 p_{r+1} S_{n-k-1} + p_0^2 p_{r+2} S_{n-k-2} + p_0^3 p_{r+3} S_{n-k-3} + \dots \\ & \qquad \dots + p_0^{n-k-1} p_{r+n-k-1} S_1 + p_0^{n-k} p_{r+n-k}^{r+n-k}, \\ 2) & -T_{r,k} = \frac{n-r}{n} p_r \frac{S'_{n-k}}{n-k} + p_0 p_{r+1} \frac{S'_{n-k-1}}{n-k-1} + p_0^2 p_{r+2} \frac{S'_{n-k-2}}{n-k-2} + p_0^3 p_{r+3} \frac{S'_{n-k-3}}{n-k-3} + \dots \\ & \qquad \dots + p_0^{n-k-1} p_{r+n-k-1} \frac{S'}{1} + p_0^{n-k} p_{r+n-k} \{\log p_0^{r+n-k-1} p_{r+n-k})\}', \end{cases}$$

si vero $r > k$

$$19. \begin{cases} 1) & -R_{r,k} = \frac{n-r}{n} p_r S_{n-k} + p_0 p_{r+1} S_{n-k-1} + p_0^2 p_{r+2} S_{n-k-2} + p_0^3 p_{r+3} S_{n-k-3} + \dots \\ & \qquad \dots + p_0^{n-r} p_n S_{r-k}, \\ 2) & -T_{r,k} = \frac{n-r}{n} p_r \frac{S'_{n-k}}{n-k} + p_0 p_{r+1} \frac{S'_{n-k-1}}{n-k-1} + p_0^2 p_{r+2} \frac{S'_{n-k-2}}{n-k-2} + p_0^3 p_{r+3} \frac{S'_{n-k-3}}{n-k-3} + \dots \\ & \qquad \dots + p_0^{n-r} p_n \frac{S'_{r-k}}{r-k}. \end{cases}$$

Notum autem est et patet ex aequationibus (14.) functionem ipsius x rationalem $\overset{n}{\underset{1}{\Sigma}}_i y_i^\nu$ generaliter gaudere denominatore p_0^ν, vel, quod idem valet $p_0^\nu \overset{n}{\underset{1}{\Sigma}}_i y_i^\nu = S_\nu$, ipsius x esse functionem integram generaliter per p_0 non divisibilem; contra vero potestatem ipsius p_0, quae denominatorem functionis rationalis $\overset{n}{\underset{1}{\Sigma}}_i p_i^\nu$ constituit, inferiorem esse quam ν^{ta}, quoties polynomiorum $p_1, p_2, p_3, \dots p_{n-1}$ quae in aequatione $\varphi(x, y) = 0$ coëfficientium locum tenent, aliquae, in quorum tamen numero ipsum p_1 esse debet, aut absint, aut per potestatem ipsius p_0 sint divisibiles. Quibus casibus specialibus missis factis sequitur, functiones $R_{r,k}$ et $T_{r,k}$ ipsius x integras per p_0 generaliter non divisibiles esse, ideoque $(n-k)$ minimum esse numeri integri positivi λ valorem, qui posito $M_k = A_k p_0^\lambda$ potestatem ipsius p_0 e denominatore functionis $Q_{r+1,k}$ exterminat; q. e. d.

3.

Posito

$$\frac{d \overset{n-1}{\underset{1}{\Sigma}}_k M_k \left(y^{n-k} - \frac{1}{n} \overset{n}{\underset{1}{\Sigma}}_i y_i^{n-k}\right)}{dx} = \frac{\overset{n-1}{\underset{1}{\Sigma}}_r N_{r+1} y^{n-r-1}}{\varphi'(y)},$$

invenimus

$$20. \quad N_{r+1} =$$

$$\overset{n-1}{\underset{1}{\Sigma}}_i \left\{(p_0 y_i^r + p_1 y_i^{r-1} + \dots + p_{r-1} y_i + p_r) - \frac{n-r}{n} p_r\right\} \{M_1 y_i^{n-1} + M_2 y_i^{n-2} + \dots + M_{n-1} y_i\}',$$

et scimus, posito $N_{r+1} = \overset{n-1}{\underset{1}{\Sigma}}_k (M'_k G_{r,k} + M_k H_{r,k})$, pro omnibus indicum r et k

valoribus $1, 2, 3, \ldots n-1$ fieri $G_{r,k}$ functionem rationalem polynomiorum p_m, $H_{r,k}$ functionem rationalem eorundem p_m et derivatorum p'_m, et denominatores functionum $G_{r,k}$ et $H_{r,k}$ esse potestates ipsius p_0. Sunt enim e paragrapho antecedenti

$$G_{r,k} = \frac{R_{r,k}}{p_0^{n-k}}, \qquad H_{r,k} = (n-k)\frac{p_0 T_{r,k} - p'_0 R_{r,k}}{p_0^{n-k}}.$$

Formam functionum ipsius x rationalium M_k ad arbitrium determinare licet; statuamus igitur

$$21. \qquad M_k = a_{1,k}B_1 + a_{2,k}B_2 + a_{3,k}B_3 + \ldots + a_{n-1,k}B_{n-1},$$

ubi $B_1, B_2, B_3, \ldots B_{n-1}$ designant functiones ipsius x rationales quaslibet et $a_{v,k}$ [pro omnibus indicum vel k valoribus $1, 2, 3, \ldots n-1$] functiones integras polynomiorum p_m ita comparandas, ut, posito

$$N_{r+1} = \sum_1^{n-1}{}_v (B'_v I_{r,v} + B_n K_{r,v})$$

ipsae $I_{r,v}$ et $K_{r,v}$ singulis indicum r et v valoribus $1, 2, 3, \ldots n-1$ respondentes fiant functiones integrae polynomiorum p_m et derivatorum p'_m, eaeque dimensionis quam minimae. Quam tamen dimensionem infra secundam decrescere non posse, patet e valoribus functionum

$$G_{r,k} = \frac{R_{r,k}}{p_0^{n-k}}, \qquad H_{r,k} = (n-k)\frac{p_0 T_{r,k} - p'_0 R_{r,k}}{p_0^{n-k+1}}$$

ope aequationum (18.) et (19.) exhibitis.

Functiones $a_{v,k}$ inventuris usu veniunt aequationes (14. 1.) et (16. 1.). Quum enim exhibeant

$$22. \qquad \sum_1^n{}_i (p_0 y_i^v + p_1 y_i^{v-1} + \ldots + p_{v-1} y_i) = -v p_v,$$

$$23. \qquad \sum_n^1{}_i p_0 y'_i (p_0 y_i^{v-1} + p_1 y_i^{v-2} + \ldots + p_{v-1}) = p_v p'_0 - p_0 q'_v,$$

docent, functiones polynomiorum p_m rationales

$$p_0 \sum_1^n{}_i y_i^v, \quad p_1 \sum_1^n{}_i y_i^{v-1}, \quad p_2 \sum_1^n{}_i y_i^{v-2}, \quad \ldots, \quad p_{v-1} \sum_1^n{}_i y_i,$$

aeque ac functiones eorundem p_m et derivatorum p'_m rationales

$$p_0^2 \sum_1^n{}_i y_i^{v-1} y'_i, \quad p_0 p_1 \sum_1^n{}_i y_i^{v-2} y'_i, \quad p_0 p_2 \sum_1^n{}_i y_i^{v-3} y'_i, \quad \ldots, \quad p_0 p_{v-1} \sum_1^n{}_i y'_i,$$

in quibus potestates ipsius p_0, inde a $(v-1)^{ta}$ usque ad primam, denominatorum locum tenent, tales esse, quarum summa fiat integra per p_0 non divisibilis. Unde recte suspicaris, ad finem propositum perventum iri, posito

$$24. \qquad \sum_1^{n-1} M_k y^{n-k} = \sum_1^{n-1}{}_v B_v (p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \ldots + p_{v-1} y),$$

ideoque

$$25. \quad \begin{cases} M_1 = p_0 B_{n-1}, \\ M_2 = p_1 B_{n-1} + p_0 B_{n-2}, \\ M_3 = p_2 B_{n-1} + p_1 B_{n-2} + p_0 B_{n-3}, \\ M_4 = p_3 B_{n-1} + p_2 B_{n-2} + p_1 B_{n-3} + p_0 B_{n-4}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ M_{n-1} = p_{n-2} B_{n-1} + p_{n-3} B_{n-2} + p_{n-4} B_{n-3} + p_{n-5} B_{n-4} + \dots + p_0 B_1. \end{cases}$$

Brevitatis causa ponamus

$$P_v(x,y) = p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \dots + p_{v-1} y + p_v,$$

fit ex aequatione (22.)

$$26. \quad \sum_1^n {}_i \{P_v(x,y_i) - p_v\} = -v p_v, \quad \text{sive} \quad \sum_1^n {}_i P_v(x,y_i) = (n-v) p_v$$

et ex aequatione (24.)

$$\sum_1^{n-1} {}_k M_k y^{n-k} = \sum_1^{n-1} {}_v B_v \{P_v(x,y) - p_v\},$$

ideoque

$$\sum_1^{n-1} {}_k M_k \Big(y^{n-k} - \frac{1}{n} \sum_1^n {}_i y_i^{n-k}\Big) = \sum_1^{n-1} {}_v B_v \Big\{P_v(x,y) - \frac{n-v}{n} p_v\Big\}.$$

Habemus igitur

$$27. \quad \frac{d \sum_1^{n-1} {}_v B_v \Big\{P_v(x,y) - \frac{n-v}{n} p_v\Big\}}{dx} = \frac{\sum_1^{n-1} {}_r N_{r+1} y^{n-r-1}}{\varphi'(y)}$$

et

$$28. \quad \begin{cases} N_{r+1} = \sum_1^n {}_i \Big\{P_r(x,y_i) - \frac{n-r}{n} p_r\Big\} \Big\{\sum_1^{n-1} {}_k M_k y^{n-k}\Big\}' \\ \quad\quad = \sum_1^n {}_i \Big\{P_r(x,y_i) - \frac{n-r}{n} p_r\Big\} \Big\{\sum_1^{n-1} {}_v B_v [P_v(x,y_i) - p_v]\Big\}', \end{cases}$$

et posito ut supra

$$29. \quad N_{r+1} = \sum_1^{n-1} {}_v \{B_v I_{r,v} + B_v K_{r,v}\},$$

demonstrandum est, functiones $I_{r,v}$ et $K_{r,v}$, alteram $I_{r,v}$ polynomiorum p_m alteram $K_{r,v}$ eorundem p_m et derivatorum p'_m fieri integras.

Sunt autem, quia $\sum_1^n {}_i P_v(n,y_i) = (n-v) p_v$,

$$30. \quad \begin{cases} 1) \; I_{r,v} = \sum_1^n {}_i P_r(x,y_i) P_v(x,y_i) - \frac{(n-r)(n-v)}{n} p_r p_v, \\ 2) \; K_{r,v} = \sum_1^n {}_i P_r(x,y_i) [P_v(x,y_i)]' - \frac{(n-r)(n-v)}{n} p_r p'_v \end{cases}$$

e quibus sequitur, fieri

$$31. \quad I_{r,v} = I_{v,r}, \quad K_{r,v} + K_{v,r} = I'_{r,v} = I'_{v,r}.$$

Brevitatis causa scribamus P_v, P'_v loco ipsarum $P_v(x, y)$, $\{P_v(x, y)\}'$, erunt identice

$$32.\quad \begin{cases} P_v = P_v, \\ y\,P_v = P_{v+1} - p_{v+1}, \\ y^2 P_v = P_{v+2} - p_{v+1}y - p_{v+2}, \\ y^3 P_v = P_{v+3} - p_{v+1}y^2 - p_{v+2}\,y - p_{v+3}, \\ \cdots\cdots\cdots\cdots \\ y^r P_v = P_{v+r} - p_{v+1}\,y^{r-1} - p_{v+2}\,y^{r-2} - p_{v+3}\,y^{r-3} - \cdots - p_{v+r}; \end{cases}$$

eodemque modo

$$33.\quad \begin{cases} P'_v = P'_v, \\ y\,P'_v = P'_{v+1} - y'P_v - p'_{v+1}, \\ y^2 P'_v = P'_{v+2} - 2y'P_{v+1} - p'_{v+1}y - p'_{v+2} \qquad + y'p_{v+1}, \\ y^3 P'_v = P'_{v+3} - 3y'P_{v+2} - p'_{v+1}y^2 - p'_{v+2}y - p'_{v+3} + y'\{p_{v+1}y + 2p_{v+2}\}, \\ \cdots\cdots\cdots\cdots \\ y^r P'_v = P'_{v+r} - r y' P_{v+r+1} - p'_{v+1}\,y^{r-1} - p'_{v+2}\,y^{r-2} - p'_{v+3}\,y^{r-3} - \cdots\cdots \\ \qquad \cdots\cdots - p'_{v+r} + y'\{p_{v+1}y^{r-2} + 2p_{v+2}y^{r-3} + \cdots + (r-1)p_{v+r-1}\}. \end{cases}$$

Unaquaeque enim aequationum (32.) ope aequationis identicae $y\,P_v = P_{v+1} - p_{v+1}$ unaquaeque autem aequationum (33.) ope aequationis identicae $y\,P'_v = P'_{v+1} - y'P_v - p'_{v+1}$ ex antecedenti prodit, per y multiplicatione facta.

Aequationum (32.) et (33.) prima per p_r, secunda per $p_{r-1}, \ldots, (m+1)^{ta}$ per p_{r-m} denique $(r+1)^{ta}$ per p_0 multiplicatis, atque aequationibus utriusque systematis post multiplicationem additis, prodeunt e systemate (32.)

$$34.\quad \begin{cases} 1)\quad P_r P_v = p_r P_v + p_{r-1}P_{v+1} + p_{r-2}P_{v+2} + \cdots + p_0 P_{v+r} \\ \qquad\qquad - p_{v+1}P_{r-1} - p_{v+2}P_{r-2} - \cdots - p_{v+r}P_0, \\ \text{vel etiam} \\ 2)\quad P_v P_r = p_v P_r + p_{v-1}P_{r+1} + p_{v-2}P_{r+2} + \cdots + p_0 P_{r+v} \\ \qquad\qquad - p_{r+1}P_{v-1} - p_{r+2}P_{v-2} - \cdots - p_{r+v}P_0, \end{cases}$$

e systemate (33.) autem

$$35.\quad \begin{cases} 1)\quad P_r P'_v = p_r P'_v + p_{r-1}P'_{v+1} + p_{r-2}P'_{v+2} + \cdots + p_0 P'_{v+r} \\ \qquad\qquad - p'_{v+1}P_{r-1} - p'_{v+2}P_{r-2} - \cdots - p'_{v+r}P_0 \\ \qquad\qquad + y'\{p_{v+1}P_{r-2} + 2p_{v+2}P_{r-3} + \cdots + (r-1)p_{v+r-1}P_0\} \\ \qquad\qquad - y'\{p_{r-1}P_{v+2}p_{r-2}P_{v+1} + \cdots + (r-1)p_1 P_{v+r-2} + r p_0 P_{v+r-1}\}, \\ \text{vel etiam} \\ 2)\quad P_r P'_v = p'_v P_r + p'_{v-1}P_{r+1} + p'_{v-2}P_{r+1} + \cdots + p'_0 P_{r+v} \\ \qquad\qquad - p_{r+1}P'_{v-1} - p_{r+2}P'_{v-2} - \cdots - p_{r+v}P'_0 \\ \qquad\qquad + y'\{p_{v-1}P_{r+2}p_{v-2}P_{r+1} + \cdots + (v-1)p_1 P_{r+v-2} + v p_0 P_{r+v-1}\} \\ \qquad\qquad - y'\{p_{r+1}P_{v-2} + 2p_{r+2}P_{v-3} + \cdots + (v-1)p_{r+v-1}P_0\}. \end{cases}$$

in quibus aequationibus symmetriae causa scripsimus P_0 loco ipsius p_0, cui aequalis est. Aequatio (34. 2.) ex ipsa (34. 1.) provenit indicibus v et r inter se permutatis, eo enim pars sinistra non mutatur, ideoque etiam pars dextra eadem manere debet. Quod sibi poscit, ut summa terminorum, quibus aequationum (34. 1.) et (34. 2.) partes dextrae altera alteram excedant, identice evanescat; et revera, si $v > r$, aequationis (34. 2.) pars dextra excedit partem dextram ipsius (34. 2.) terminis

$$p_v P_r + p_{v-1} P_{r+1} + p_{v-2} P_{r+2} + \dots + p_{r+2} P_{v-2} + p_{r+1} P_{v-1}$$
$$- p_{r+1} P_{v-1} - p_{r+2} P_{v-2} + \dots + p_{v-2} P_{r+2} + p_{v-1} P_{r+1} - p_v P_r$$

se invicem destruentibus.

Aequatio (35. 2.) variis modis exhibetur; simplicissime autem, ubi in aequatione identica

$$P_r P'_v = \{P_r P_v\}' - P_v P'_r$$

substituuntur loco ipsius $P_r P_v$ valor aequationis (34. 2.), loco ipsius $P_v P'_r$ autem valor quem aequatio (35. 1.) praebet indicibus v et r inter se permutatis. Quia in aequationibus (34. 1.) et (35. 1) index r, in ipsis (34. 2.) et (35. 2.) autem index v usque ad 0 comminuitur, has ubi $v > r$, illas vero ubi $r > v$, calculo adhibere convenit. Adnotandum etiam est in aequationibus et antecedentibus et sequentibus quantitates p_m ipsi 0 aequales poni debere, quoties index m aut negativus sit aut numerum n superet, unde etiam quantitates P_v evanescunt, quoties v negativus aut maior quam $n-1$. Habetur autem, quia $u-y$ expressionem $\varphi(x, u) = p_0 u^n + p_1 u^{n-1} + p_2 u^{n-2} + \dots + p_{n-1} u + p_n$ metitur,

$$36. \qquad \frac{\varphi(x,u)}{u-y} = P_0 u^{n-1} + P_1 u^{n-2} + P_2 u^{n-3} + \dots + P_{n-2} u + P_{n-1};$$

est enim

$$P_v = p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \dots + p_{v-1} y + p_v.$$

His praeparatis functiones $\sum_1^n{}_i P_r(x,y_i) P_v(x,y_i)$, $\sum_1^n{}_i P_r(x,y_i)[P_v(x,y_i)]'$ ideoque et ipsae $I_{r,v}$ et $K_{r,v}$ ut functiones rationales integrae polynomiorum p_m et derivatorum p'_m facillime exhibentur. Docent enim aequationes (22.) et (33.) fieri

$$\sum_1^n{}_i P_v(x,y_i) = (n-v) p_v, \qquad p_0 \sum_1^n{}_i y'_i P_v(x,y_i) = p_{v+1} p'_0 - p_0 p'_{v+1},$$

ideoque

$$37. \qquad p_{v+1} \sum_1^n{}_i y'_i P_{r-2}(x,y_i) - p_{r-1} \sum_1^n{}_i y'_i P_v(x,y_i) = p_{r-1} p'_{v+1} - p_{v+1} p'_{r-1}.$$

Quarum ope ex aequationibus (34.) et (35.) statim prodeunt

$$38.\quad I_{r,v} = \Sigma_i P_r(x,y_i) P_v(x,y_i) - \frac{(n-r)(n-v)}{n} p_r p_v$$
$$= \frac{n-v}{n} r p_r p_v - (v-r)\{p_{r-1}p_{v+1} + p_{r-2}p_{v+2} + p_{r-3}p_{v+3} + \dots + p_0 p_{v+r}\}$$
$$- 2\{p_{r-1}p_{v+1} + 2p_{r-2}p_{v+2} + 3p_{r-3}p_{v+3} + \dots + r p_0 p_{v+r}\}$$
$$= \frac{n-r}{n} v p_v p_r - (r-v)\{p_{v-1}p_{r+1} + p_{v-2}p_{r+2} + p_{v-3}p_{r+3} + \dots + p_0 p_{r+v}\}$$
$$- 2\{p_{v-1}p_{r+1} + 2p_{v-2}p_{r+2} + 3p_{v-3}p_{r+3} + \dots + v p_0 p_{r+v}\}$$

$$39.\quad K_{r,v} = \sum_1^n {}_i P_r(x,y)[P_v(x,y_i)]' - \frac{(n-r)(n-v)}{n} p_r p_v'$$
$$= \frac{n-v}{n} r p_r p_v' - (v-r)\{p_{r-1}p_{v+1}' + p_{r-2}p_{v+2}' + p_{r-3}p_{v+3}' + \dots + p_0 p_{v+r}'\}$$
$$- (p_{r-1}p_{v+1})' - 2(p_{r-2}p_{v+2})' - 3(p_{r-3}p_{v+3})' - \dots - r(p_0 p_{v+r})'$$
$$= \frac{n-r}{n} v p_v' p_r - (r-v)\{p_{v-1}' p_{r+1} + p_{v-2}' p_{r+2} + p_{v-3}' p_{r+3} + \dots + p_0' p_{r+v}\}$$
$$- (p_{v-1}p_{r+1})' - 2(p_{v-2}p_{r+2})' - 3(p_{v-3}p_{r+3})' - \dots - v(p_0 p_{r+v})',$$

ut functiones integrae polynomiorum p_m et derivatorum p_m' dimensionis secundae.

4.

Formulae paragraphi antecedentis adhuc valent, si $p_0, p_1, p_2, \dots p_n$, $B_1, B_2, B_3, \dots B_{n-1}$; $N_2, N_3, \dots N_n$ sunt functiones quaelibet ipsius x, ita tantum circumscriptae, ut ambiguitatem non permittant. Functiones tamen p_m semper ita comparatae esse supponuntur, ut aequatio $\varphi(x,y)=0$ radicibus aequalibus non gaudeat. Paragrapho igitur antecedenti duo demonstrata sunt theoremata sequentia, alterum alterius inversum.

Theorema I.

Si designatur per y radix quaelibet aequationis

$$\varphi(x,y) = 0 = p_0 y^n + p_1 y^{n-1} + p_2 y^{n-2} + \dots + p_{n-1} y + p_n$$
$$= p_0(y-y_1)(y-y_2)(y-y_3)\dots(y-y_n)$$

radicibus aequalibus non gaudentis, per $p_0, p_1, p_2, \dots p_n$, $B_1, B_2, \dots B_{n-1}$ functiones quaelibet ipsius x ita circumscriptae, ut ambiguitatem non permittant, erit, posito

$$P_v(x,y) = p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \dots + p_{v-1} y + p_v:$$

$$\frac{d\sum_1^{n-1}{}_v B_v\left\{P_v(x,y) - \frac{n-v}{n}p_v\right\}}{dx} = \frac{\sum_1^{n-1}{}_r N_{r+1} y^{n-r-1}}{\varphi'(y)},$$

$$N_{r+1} = \sum_1^{n-1}{}_v (B_v' I_{r,v} + B_v K_{r,v}),$$

ubi pro omnibus indicum r et v valoribus 1, 2, 3, ... $n-1$ fiunt

$$40.\quad I_{r,v} = \frac{n-v}{n} r p_r p_v - \sum_1^r{}_m (v-r+2m) p_{r+m} p_{v+m}$$
$$= \frac{n-r}{n} v p_v p_r - \sum_1^v{}_m (r-v+2m) p_{v-m} p_{r+m},$$

$$41.\quad K_{r,v} = \frac{n-v}{n} r p_r p'_v - \sum_1^r{}_m \{(v-r+2m) p_{r-m} p'_{v+m} - m(p_{r-m} p'_{v+m} - p_{v+m} p'_{r-m})\}$$
$$= \frac{n-r}{n} v p'_v p_r - \sum_1^v{}_m \{(r-v+2m) p'_{v-m} p_{r+m} + m(p_{v-m} p'_{r+m} - p_{r+m} p'_{v-m})\},$$

ideoque

$$I_{r,v} = I_{v,r}, \qquad K_{r,v} + K_{v,r} = I'_{r,v} = I'_{v,r}.$$

Theorema II.

Proposito inter $n-1$ variabiles B_1, B_2, B_3, ... B_{n-1} et variabilem x systemate $n-1$ aequationum differentialium linearium primi ordinis

$$42.\quad \begin{cases} \sum_1^{n-1}{}_v (B'_v I_{1,v} + B_v K_{1,v}) = N_2, \\ \sum_1^{n-1}{}_v (B'_v I_{2,v} + B_v K_{2,v}) = N_3, \\ \sum_1^{n-1}{}_v (B'_v I_{3,v} + B_v K_{3,v}) = N_4, \\ \dots\dots\dots\dots\dots\dots \\ \sum_1^{n-1}{}_v (B'_v I_{n-1,v} + B_v K_{n-1,v}) = N_n, \end{cases}$$

in quibus $I_{r,v}$ et $K_{r,v}$ pro omnibus indicum r et v valoribus 1, 2, 3, ... $n-1$ definitae sunt per aequationes (40.) et (41.), siquidem quantitates p_m ipsi 0 aequales ponuntur, quoties index m aut negativus est, aut numerum n superat; N_2, N_3, ... N_n autem aeque ac ipsae p_0, p_1, p_2, ... p_n functiones quaelibet datae ipsius x sunt, ita tantum circumscriptae, ut ambiguitatem non permittant, positis

$$p_0 y^n + p_1 y^{n-1} + p_2 y^{n-2} + \dots + p_{n-1} y + p_n = p_0(y-y_1)(y-y_2)(y-y_3)\dots(y-y_n)$$
$$= \varphi(x,y),$$
$$p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \dots + p_{v-1} y + p_v = P_v(x,y).$$

locum tenebunt $n-1$ integralium completorum systematis (42.) quaelibet $n-1$ ex n aequationibus

$$43.\quad\begin{cases}
\sum_1^{n-1} B_r \left\{P_r(x,y_1) - \frac{n-r}{n} p_r\right\} = \int_{a_1}^{x} \frac{\sum_1^{n-1} N_{r+1} y_1^{n-r-1}}{\varphi'(y_1)}\, dx, \\
\sum_1^{n-1} B_r \left\{P_r(x,y_2) - \frac{n-r}{n} p_r\right\} = \int_{a_2}^{x} \frac{\sum_1^{n-1} N_{r+1} y_2^{n-r-1}}{\varphi'(y_2)}\, dx, \\
\sum_1^{n-1} B_r \left\{P_r(x,y_3) - \frac{n-r}{n} p_r\right\} = \int_{a_3}^{x} \frac{\sum_1^{n-1} N_{r+1} y_3^{n-r-1}}{\varphi'(y_3)}\, dx, \\
\dots\dots\dots\dots\dots\dots \\
\sum_1^{n-1} B_r \left\{P_r(x,y_n) - \frac{n-r}{n} p_r\right\} = \int_{a_n}^{x} \frac{\sum_1^{n-1} N_{r+1} y_n^{n-r-1}}{\varphi'(y_n)}\, dx.
\end{cases}$$

in quibus $a_1, a_2, a_3, \dots a_n$ designant constantes arbitrarias conditioni obnoxias

$$44.\quad 0 = \int_{a_1}^{a_i} \frac{\sum_1^{n-1} N_{r+1} y_1^{n-r-1}}{\varphi'(y_1)}\, dx + \int_{a_2}^{a_i} \frac{\sum_1^{n-1} N_{r+1} y_2^{n-r-1}}{\varphi'(y_2)}\, dx + \dots$$

$$\dots\dots + \int_{a_n}^{a_i} \frac{\sum_1^{n-1} N_{r+1} y_n^{n-r-1}}{\varphi'(y_n)}\, dx,$$

in qua a_i designat quamlibet e n quantitatibus $a_1, a_2, a_3, \dots a_n$. Aequatio (44.) respectu harum n quantitatum symmetrica est; quod apparet, si ad eam additur aequatio notissima $\sum_1^n{}_i \int_{a_i}^{c} \frac{\sum_1^{n-1} N_{r+1} y_i^{n-r-1}}{\varphi'(y_i)}\, dx = 0$, in qua c designat constantem datam, e. g. zero.

Pro $n=2$ theorema II. in sequens abit e primis elementis calculi infinitesimalis notissimum: „aequationis differentialis

$$B_1'(\tfrac{1}{2}p_1^2 - 2p_0p_2) + B_1(\tfrac{1}{2}p_1p_1' - (p_0p_2)') = N_2$$

(in quam aequationes (42.) pro $n=2$ corruunt) integrale esse

$$\tfrac{1}{2}B_1\sqrt{(p_1^2 - 4p_0p_2)} = \int_{a_1}^{x} \frac{N_2\, dx}{\sqrt{(p_1^2 - 4p_0p_2)}}.$$

Fiunt enim pro $n=2$:

$$\varphi(x,y) = p_0y^2 + p_1y + p_2 = p_0(y-y_1)(y-y_2),$$

$$\sum_1^{n-1} B_r\left(P_r(x,y) - \frac{n-r}{n}p_r\right) = B_1(p_0y + \tfrac{1}{2}p_1) = \pm B_1\tfrac{1}{2}\sqrt{(p_1^2 - 4p_0p_2)}.$$

5.

Duo theoremata, modo exposita, sibi poscunt, ut aequatio $\varphi(x,y)=0$ pro indefinito ipsius x valore radicibus aequalibus y, vel quod idem est, cum aequatione $\varphi'(y)=0$ communibus non gaudeat. Proficiscitur autem theorema II. non ab ipsa aequatione $\varphi(x,y)=0$, sed a systemate $n-1$ aequationum differentialium (42.), ad quod in theoremate I. ex illa perveneramus. Unde, si functiones p_m eius modi sunt, ut aequationi satisfiat, quae variabili y eliminata ex aequationibus $\varphi(x,y)=0$, $\varphi'(y)=0$ provenit, etiam ipsae aequationes (42.) repugnantiam aliquam continebunt. Quae ut appareat, demonstremus, aequationem, cui a functionibus p_m satisfieri non debet, eandem esse cum ea, quam ex aequationibus (42.) lucramur, Determinante, e $(n-1)^2$ quantitatibus $I_{r,v}$ conflato, ipsi 0 aequali posito; siquidem more a geometris celeberrimis accepto Determinantis, e $(n-1)^2$ elementis $I_{r,v}$ conflati, nomen tribuitur „aggregato

$$45.\quad L = \Sigma \pm I_{1,1}\, I_{2,2}\, I_{3,3} \ldots . I_{n-1,n-1},$$

„$1.2.3 \ldots . n-1$ terminorum, qui e termino $I_{1,1}\, I_{2,2}\, I_{3,3} \ldots . I_{n-1,n-1}$ prodeunt „indicibus omnibus aut prioribus aut posterioribus omni modo inter se permu-„tatis, singulis terminis praefixo signo aut $+$ aut $-$ ea lege, ut binis ex in-„dicibus aut prioribus aut posterioribus inter se commutatis, tota expressio L „valorem oppositum induat."

Ubi enim ex aequationibus (42.) functiones derivatae $B'_v = \frac{dB_v}{dx}$ per ipsas $B_1, B_2, \ldots . B_n$ et x exprimuntur, prodeunt aequationes

$$46.\quad dx : dB_1 : dB_2 : \ldots . : dB_{n-1} = L : \beta_1 : \beta_2 : \ldots . : \beta_{n-1},$$

in quibus $\beta_1, \beta_2, \ldots . \beta_{n-1}$ sunt functiones datae ipsarum $B_1, B_2, \ldots . B_n$ et x; atque ut aequationes (46.) vim habeant systematis $n-1$ aequationum differentialium, e quibus $n-1$ variabiles $B_1, B_2, \ldots . B_n$ functiones ipsius x exhibeantur, L vera functio ipsarum x et $B_1, B_2, \ldots . B_n$ esse debet, neque expressio pro indefinitis valoribus earum identice evanescens.

Aequatio autem

$$46_1.\quad L = \Sigma \pm I_{1,1}\, I_{2,2}\, I_{3,3} \ldots . I_{n-1,n-1} = 0$$

ipsa prodit ex aequationibus $\varphi(x,y)=0$, $\varphi'(y)=0$ variabili y eliminata, siquidem eliminatio perficitur secundum methodum a clarissimo *Bézout* inventam, quam clarissimus *Jacobi* in commentatione egregia „De eliminatione variabilis e duabus aequationibus algebraicis" (Diarii Crelliani tomo XV. inserta) pervestigavit, eiusque proprietates admirabiles luculentissime exposuit. Methodus illa haec est:

Propositis duabus aequationibus algebraicis gradus n^{ti}

$$46. \begin{cases} 1) & f(y) = a_0 y^n + a_1 y^{n-1} + a_2 y^{n-2} + \dots + a_{n-1} y + a_n = 0, \\ 2) & F(y) = b_0 y^n + b_1 y^{n-1} + b_2 y^{n-2} + \dots + b_{n-1} y + b_n = 0, \end{cases}$$

pro radice y, quae utrique satisfacit, n expressiones

$$47. \begin{cases} m_0 = b_0 f(y) - a_0 F(y), \\ m_1 = (b_0 y + b_1) f(y) - (a_0 y + a_1) F(y), \\ m_2 = (b_0 y^2 + b_1 y + b_2) f(y) - (a_0 y^2 + a_1 y + a_2) F(y), \\ \dots \\ m_{n-2} = (b_0 y^{n-2} + b_1 y^{n-3} + b_2 y^{n-4} + \dots + b_{n-3} y + b_{n-2}) f(y) \\ \qquad - (a_0 y^{n-2} + a_1 y^{n-3} + a_2 y^{n-4} + \dots + a_{n-3} y + a_{n-2}) F(y), \\ m_{n-1} = (b_0 y^{n-1} + b_1 y^{n-2} + b_2 y^{n-3} + \dots + b_{n-2} y + b_{n-1}) f(y) \\ \qquad - (a_0 y^{n-1} + a_1 y^{n-2} + a_2 y^{n-3} + \dots + a_{n-2} y + a_{n-1}) F(y), \end{cases}$$

quae sponte ad gradum $(n-1)^{tum}$ descendunt omnes ipsi 0 aequales fiunt, unde si symmetrice omnes termini a factore y liberi per y^0 multiplicentur, positis

$$48. \begin{cases} m_0 = a_{0,0} y^{n-1} + a_{1,0} y^{n-2} + a_{2,0} y^{n-3} + \dots + a_{n-1,0} y^0, \\ m_1 = a_{0,1} y^{n-1} + a_{1,1} y^{n-2} + a_{2,1} y^{n-3} + \dots + a_{n-1,1} y^0, \\ m_2 = a_{0,2} y^{n-1} + a_{1,2} y^{n-2} + a_{2,2} y^{n-3} + \dots + a_{n-1,2} y^0, \\ \dots \\ m_{n-1} = a_{0,n-1} y^{n-1} + a_{1,n-1} y^{n-2} + a_{2,n-1} y^{n-3} + \dots + a_{n-1,n-1} y^0, \end{cases}$$

pro radice y aequationibus $0 = f(y)$ et $0 = F(y)$ communi habentur n aequationes

$$m_0 = 0, \quad m_1 = 0, \quad m_2 = 0, \quad \dots \quad m_{n-1} = 0,$$

e quibus, ipsis $y^0, y^1, y^2, \dots y^{n-1}$ eliminatis, prodit Determinans

$$49. \quad \Delta = \Sigma \pm a_{0,0}\, a_{1,1}\, a_{2,2} \dots a_{n-1,n-1} = 0;$$

quod quum et respectu coëfficientium a_m et respectu coëfficientium b_m ad n^{tam} dimensionem ascendat, patet e theoremate notissimo cl. *Euleri*, aequationem (49.) esse finalem genuinam, quae ex aequationibus propositis (46.) $f(y)=0$, $F(y)=0$ variabili y eliminata provenit, factore superfluo non affectam. Sunt enim quantitates $a_{r,v}$, et respectu coëfficientium a_m et respectu coëfficientium b_m, lineares atque

$$50. \begin{cases} a_{v,r} = a_{v+1} b_r + a_{v+2} b_{r-1} + a_{v+3} b_{r-2} + \dots + a_{v+1+r} b_0 \\ \qquad - b_{v+1} a_r - b_{v+2} a_{r-1} - b_{v+3} a_{r-2} - \dots - b_{v+1+r} a_0 \\ = a_{r,v} = a_{r+1} b_v + a_{r+2} b_{v-1} + a_{r+3} b_{v-2} + \dots + a_{r+1+v} b_0 \\ \qquad - b_{r+1} a_v - b_{r+2} a_{v-1} - b_{r+3} a_{v-2} - \dots - b_{r+1+v} a_0, \end{cases}$$

quia, si $v > r$, expressio altera priorem excedit terminis

$$a_{r+1} b_v + a_{r+2} b_{v-1} + \dots + a_v b_{r+1} - b_{r+1} a_v - b_{r+2} a_{v-1} - \dots - b_v a_{r+1}$$

sponte se destruentibus. Qui valores ipsarum $\alpha_{r,v} = \alpha_{v,r}$ pro omnibus indicum r et v valoribus locum habent, siquidem coëfficientes a_m et b_m ipsi 0 aequales ponuntur, ubi index m numerum n superat, aut negativus est.

6.

Ut omnia in promtu sint, quibus infra nobis opus erit, formulas etiam sequentes e commentatione laudata hoc loco colligamus.

Ponamus, aequationibus (48.) resolutis, fieri

$$51.\quad \begin{cases} \Delta y^{n-1} = A_{0,0} m_0 + A_{0,1} m_1 + A_{0,2} m_2 + \dots + A_{0,n-1} m_{n-1}, \\ \Delta y^{n-2} = A_{1,0} m_0 + A_{1,1} m_1 + A_{1,2} m_2 + \dots + A_{1,n-1} m_{n-1}, \\ \Delta y^{n-3} = A_{2,0} m_0 + A_{2,1} m_1 + A_{2,2} m_2 + \dots + A_{2,n-1} m_{n-1}, \\ \dots\dots\dots\dots\dots\dots \\ \Delta y^{0} = A_{n-1,0} m_0 + A_{n-1,1} m_1 + A_{n-1,2} m_2 + \dots + A_{n-1,n-1} m_{n-1}, \end{cases}$$

erit propter $\alpha_{r,v} = \alpha_{v,r}$ etiam $A_{r,v} = A_{v,r}$, atque, ubi n aequationum $m_0 = 0$, $m_1 = 0$, $m_2 = 0$, ... $m_{n-1} = 0$, quas pro radice y aequationibus (46.) communi locum habere vidimus, quaelibet $m_v = 0$ reiicitur, e $n-1$ reliquis exhibentur rationes potestatum descendentium huius radicis

$$52.\quad y^{n-1} : y^{n-2} : y^{n-3} : \dots : y^1 : y^0 = A_{0,v} : A_{1,v} : A_{2,v} : \dots : A_{n-2,v} : A_{n-1,v},$$

ideoque

$$y^{n-1-r} : y^{n-1-v_1} = A_{r,v} : A_{v_1,v}$$

et, posito in aequationibus (52.) v_1 loco ipsius v,

$$y^{n-1-v} : y^{n-1-r_1} = A_{v,v_1} : A_{r_1,v_1};$$

unde, altera proportione in alteram ducta, propter $A_{v_1,v} = A_{v,v_1}$, prodit

$$53.\quad y^{n-1-r} . y^{n-1-v} : y^{n-1-r_1} . y^{n-1-v_1} = A_{r,v} : A_{r_1,v_1}.$$

Quoties igitur $r+v = r_1+v_1$, erit $A_{r,v} = A_{r_1,v_1}$ sive $A_{r,v} - A_{r_1,v_1} = 0$. Expressio autem $A_{r,v} - A_{r_1,v_1}$ est functio rationalis integra coëfficientium a_m et b_m atque ascendit et harum et illarum respectu ad dimensionem $(n-1)^{\text{tam}}$; quae, quum minor sit quam dimensio n^{ta}, ad quam aequatio finalis genuina $\Delta = 0$, respectis coëfficientibus utriusque aequationis (46.), assurgit, e theoremate notissimo $A_{r,v} - A_{r_1,v_1}$ identice evanescere debet, sive quantitates omnes $A_{r,v}$, quibus eadem est summa indicum $r+v$, identicae sunt. Posito igitur $A_{r,v} = A_{r+v}$, videmus eam esse naturam quantitatum $\alpha_{r,v} = \alpha_{v,r}$, ut posito

$$54.\quad \begin{cases} m_0 = \alpha_{0,0} y_{n-1} + \alpha_{1,0} y_{n-2} + \alpha_{2,0} y_{n-3} + \dots + \alpha_{n-1,0} y_0, \\ m_1 = \alpha_{0,1} y_{n-1} + \alpha_{1,1} y_{n-2} + \alpha_{2,1} y_{n-3} + \dots + \alpha_{n-1,1} y_0, \\ m_2 = \alpha_{0,2} y_{n-1} + \alpha_{1,2} y_{n-2} + \alpha_{2,2} y_{n-3} + \dots + \alpha_{n-1,2} y_0, \\ \dots\dots\dots\dots\dots\dots \\ m_{n-1} = \alpha_{0,n-1} y_{n-1} + \alpha_{1,n-1} y_{n-2} + \alpha_{2,n-1} y_{n-3} + \dots + \alpha_{n-1,n-1} y_0, \end{cases}$$

aequationes inversae, quibus quantitates y_{n-1-r} per quantitates m_r exhibentur, formam sequentem induant:

$$55.\quad \begin{cases} \varDelta y_{n-1} = A_0 m_0 + A_1 m_1 + A_2 m_2 + \dots + A_{n-1} m_{n-1}, \\ \varDelta y_{n-2} = A_1 m_0 + A_2 m_1 + A_3 m_2 + \dots + A_n m_{n-1}, \\ \varDelta y_{n-3} = A_2 m_0 + A_3 m_1 + A_4 m_2 + \dots + A_{n+1} m_{n-1}, \\ \dots\dots\dots\dots\dots\dots\dots \\ \varDelta y_0 \;\; = A_{n-1} m_0 + A_n m_1 + A_{n+1} m_2 + \dots + A_{2n-2} m_{n-1}; \end{cases}$$

atque erunt

$$\alpha_{r,0} A_r + \alpha_{r,1} A_{r+1} + \alpha_{r,2} A_{r+2} + \dots + \alpha_{r,n-1} A_{r+n-1} = \varDelta,$$

et si r et v numeri diversi sunt, identice

$$\alpha_{r,0} A_v + \alpha_{r,1} A_{v+1} + \alpha_{r,2} A_{v+2} + \dots + \alpha_{r,n-1} A_{v+n-1} = 0.$$

Novo signo A_{r+v} loco ipsius $A_{r,v}$ substituto, et posito $r+v=t$, $r_1+v_1=u$, aequatio (53.) abit in sequentem

$$y^{2n-2-t} : y^{2n-2-u} = A_t : A_u.$$

Unde, quum numeris t et u valores $0, 1, 2, 3, \dots n-1$ tribuere liceat, obtinetur, quoties pro valore ipsius y aequationes $f(y)=0$ et $F(y)=0$ simul locum habent, ideoque fit $\varDelta = 0$:

$$56.\quad y^{2n-2} : y^{2n-3} : y^{2n-4} : \dots : y^1 : y^0 = A_0 : A_1 : A_2 : \dots : A_{2n-3} : A_{2n-2}.$$

Quibus rationibus substitutis in aequationes

$$y^{n-2} f(y) = 0,\quad y^{n-3} f(y) = 0,\quad y^{n-4} f(y) = 0,\quad \dots\quad y^0 f(y) = 0,$$
$$y^{n-2} F(y) = 0,\quad y^{n-3} F(y) = 0,\quad y^{n-4} F(y) = 0,\quad \dots\quad y^0 F(y) = 0,$$

habemus aequationes identicas

$$57.\quad \begin{cases} 0 = a_0 A_0 + a_1 A_1 + a_2 A_2 + \dots + a_n A_n, \\ 0 = a_0 A_1 + a_1 A_2 + a_2 A_3 + \dots + a_n A_{n+1}, \\ 0 = a_0 A_2 + a_1 A_3 + a_2 A_4 + \dots + a_n A_{n+2}, \\ \dots\dots\dots\dots\dots\dots \\ 0 = a_0 A_{n-2} + a_1 A_{n-1} + a_2 A_n + \dots + a_n A_{2n-2}; \end{cases}$$

$$58.\quad \begin{cases} 0 = b_0 A_0 + b_1 A_1 + b_2 A_2 + \dots + b_n A_n, \\ 0 = b_0 A_1 + b_1 A_2 + b_2 A_3 + \dots + b_n A_{n+1}, \\ 0 = b_0 A_2 + b_1 A_3 + b_2 A_4 + \dots + b_n A_{n+2}, \\ \dots\dots\dots\dots\dots\dots \\ 0 = b\, A_{n-2} + b_1 A_{n-1} + b_2 A_n + \dots + b_n A_{2n-2}. \end{cases}$$

Dextrae enim partes aequationum (57.) respectis quantitatibus b_m, aequationum (58.) autem respectis quantitatibus a_m tantum ad $(n-1)^{\text{tam}}$ dimensionem ascendunt, ideoque *identice* evanescere debent.

Valoribus quantitatum $m_1, m_1, m_2, \ldots\ldots m_{n-1}$ ex aequationibus (47.) substitutis, aequationes (51.) repraesentant veterem cl. *Euleri* methodum eliminationis variabilis y e duabus aequationibus algebraicis, anno 1764 in Actis Acad. Ber. Tom. XX. propositam, quae eo continetur, quod $2n$ coëfficientes binarum functionum ipsius y rationalium integrarum V_s et W_s gradus $(n-1)^{ti}$ ita determinantur, ut fiat

$$59. \quad V_s f(y) + W_s F(y) = y^s,$$

siquidem s designat quemlibet e $(2n)$ numeris $0, 1, 2, 3, \ldots\ldots 2n-1$. Hoc enim manifesto postulat resolutionem $2n$ aequationum linearium inter $2n$ incognitas, quarum denominator communis, quum respectis coëfficientibus utriusque aequationis $f(y) = 0$ et $F(y) = 0$ ad dimensionem n^{tam} ascendat, atque evanescere debeat, si $f(y)$ et $F(y)$ simul evanescunt, ipsi 0 aequalis posito praebebit aequationem finalem quaesitam, ita ut Determinanti $\varDelta$ aequalis esse debeat. Resolutio tamen illarum $2n$ aequationum linearium aequationibus (51.) iam perfecta est. Nam $(r+1)^{ta}$ aequationum (51.)

$$60. \quad \varDelta y^{n-1-r} = A_r m_0 + A_{r+1} m_1 + A_{r+2} m_2 + \ldots\ldots + A_{r+n-1} m_{n-1}$$

substituto

$$61. \quad m_v = (b_0 y^v + b_1 y^{v-1} + b_2 y^{v-2} + \ldots\ldots + b_{v-1} y + b_v) f(y) \\ - (a_0 y^v + a_1 y^{v-1} + a_2 y^{v-2} + \ldots\ldots + a_{v-1} y + a_v) F(y)$$

abit in hanc

$$62. \quad \varDelta y^{n-1-r} = \varDelta V_{n-1-r} f(y) + \varDelta W_{n-1-r} F(y),$$

in qua fiunt

$$63. \quad + \varDelta V_{n-1-r} = \sum_0^{n-1}{}_v A_{r+v} (b_0 y^v + b_1 y^{v-1} + b_2 y^{v-2} + \ldots\ldots + b_{v-1} y + b_v),$$

$$64. \quad - \varDelta W_{n-1-r} = \sum_0^{n-1}{}_v A_{r+v} (a_0 y^v + a_1 y^{v-1} + a_2 y^{v-2} + \ldots\ldots + a_{v-1} y + a_v).$$

Quibus tamen formulis, quum index r non nisi valores $0, 1, 2, 3, \ldots\ldots n-1$ permittat, functionum multiplicatricium V_s et W_s eae tantum exhibentur, quae indicis s valoribus $0, 1, 2, 3, \ldots\ldots n$ respondent. Quia autem habemus

$$a_0 y^v + a_1 y^{v-1} + a_2 y^{v-2} + \ldots\ldots + a_{v-1} y + a_v = \frac{f(y)}{y^{n-v}} - \frac{a_{v+1}}{y} - \frac{a_{v+2}}{y^2} - \ldots\ldots - \frac{a_n}{y^{n-v}},$$

$$b_0 y^v + b_1 y^{v-1} + b_2 y^{v-2} + \ldots\ldots + b_{v-1} y + b_v = \frac{F(y)}{y^{n-v}} - \frac{b_{v+1}}{y} - \frac{b_{v+2}}{y^2} - \ldots\ldots - \frac{b_n}{y^{n-v}},$$

prodeunt, aequationibus (61.) et (60.) per y^n multiplicatis,

$$65. \quad m_v y^n = y^v (a_n + a_{n-1} y + a_{n-2} y^2 + \ldots\ldots + a_{v+1} y^{n-1-v}) F(y) \\ - y^v (b_n + b_{n-1} y + b_{n-2} y^2 + \ldots\ldots + b_{v+1} y^{n-1-v}) f(y),$$

$$66. \quad \varDelta y^{2n-1-r} = \varDelta V_{2n-1-r} f(y) + \varDelta W_{2n-1-r} F(y),$$

ac fiunt

$$67.\quad -\Delta V_{2n-1-r} = \sum_{0}^{n-1}{}_{v} A_{r+v} y^v (b_n + b_{n-1} y + b_{n-2} y^2 + \dots + b_{v+1} y^{n-1-v}),$$

$$68.\quad +\Delta W_{2n-1-r} = \sum_{0}^{n-1}{}_{v} A_{r+v} y^v (a_n + a_{n-1} y + a_{n-2} y^2 + \dots + a_{v+1} y^{n-1-v}).$$

Quae valores reliquarum functionum multiplicatricium V_s et W_s indicis s valoribus n, $n+1$, $n+2$, ... $2n-1$ respondentium exhibent, quia index r iterum valores 0, 1, 2, 3, ... $n-1$ permittat. E $2n$ paribus functionum V_s, W_s $2n$ indicis s valoribus 0, 1, 2, 3, ... $2n-1$ respondentibus, functiones ipsius y rationales integrae V et W $(n-1)^{ti}$ gradus componuntur, quae, data functione ipsius y rationali integra gradus $(2n-1)^{ti}$,

$$69.\quad Q = l_0 + l_1 y + l_2 y^2 + \dots + l_{2n-2} y^{2n-2} + l_{2n-1} y^{2n-1}$$

efficiunt

$$70.\quad Vf(y) + WF(y) = Q.$$

Fiunt enim

$$71.\quad \begin{cases} V = l_0 V_0 + l_1 V_1 + l_2 V_2 + \dots + l_{2n-2} V_{2n-2} + l_{2n-1} V_{2n-1}, \\ W = l_0 W_0 + l_1 W_1 + l_2 W_2 + \dots + l_{2n-2} W_{2n-2} + l_{2n-1} W_{2n-1}. \end{cases}$$

7.

In commentatione laudata, e qua formulae paragraphi antecedentis petitae sunt, auctor clarissimus duas aequationes propositas eiusdem gradus esse supposuit, atque adnotavit, quoties altera gradus inferioris esset, in formulis illis nil mutatum iri, nisi quod coëfficientes potestatum superiorum in ea deficientium nullitati aequandae forent. Sed tum Determinans Δ aequationum (48.) ipsi 0 aequale positum non praebebit aequationem finalem *genuinam*, quae variabili y eliminata ex aequationibus $f(y) = 0$, $F(y) = 0$ provenit; erit enim respectis coëfficientibus utriusque aequationis dimensionis n^{tae}, dimensio autem aequationis finalis genuinae respectis coëfficientibus alterius aequationis gradum alterius aequare debet; unde casu graduum inaequalium aequationum propositarum $f(y) = 0$, $F(y) = 0$ aequatio finalis

$$\Delta = \Sigma \pm \alpha_{0,0} \alpha_{1,1} \alpha_{2,2} \dots \alpha_{n-1,n-1} = 0$$

factore superfluo affecta erit.

Sit aequationum (46.) altera $F(y) = 0$ gradus $(n-k)^{ti}$, ideoque $b_0 = 0$, $b_1 = 0$, $b_2 = 0$, ... $b_{k-1} = 0$, factor ille superfluus Determinantis Δ, qui manifesto erit functio rationalis integra quantitatum a_m dimensionis k^{tae} (aequatio enim finalis genuina respectis quantitatibus a_m nonnisi ad dimensionem $(n-k)^{tam}$ ascendere debet) exhibetur ope theorematis, a clarissimo *Jacobi* in commen-

tatione „De forma et proprietatibus Determinantium" (Diar. Crell. tom XXII. pag. 311) demonstrati:

„Fieri Determinans

$$72.\quad \Sigma \pm c_0^{(0)} c_1' c_2'' \ldots c_{n-1}^{(n-1)} = \Sigma \pm \gamma_0^{(0)} \gamma_1' \gamma_2'' \ldots \gamma_{k-1}^{(n-k)} \Sigma \pm g_0^{(0)} g_1' g_2'' \ldots g_{n-1}^{(n-1)},$$

„si pro valoribus 0, 1, 2, ... $k-1$ indices v sit

$$73.\quad c_r^{(v)} = \gamma_0^{(v)} g_0^{(r)} + \gamma_1^{(v)} g_1^{(r)} + \gamma_2^{(v)} g_2^{(r)} + \ldots + \gamma_{k-1}^{(v)} g_{k-1}^{(r)},$$

„pro indicis v valoribus maioribus quam $k-1$,

$$74.\quad c_r^{(v)} = g_v^{(r)}."$$

Erunt enim pro k valoribus 0, 1, 2, 3, ... $k-1$ indicis v ex aequationibus (47.) et (50.)

$$75.\quad m_v = -a_0 y^v F(y) - a_1 y^{v-1} F(y) - a_2 y^{v-2} F(y) - \ldots - a_v F(y),$$

$$76.\quad \alpha_{r,v} = -a_v b_{r+1} - a_{v-1} b_{r+2} - a_{v-2} b_{r+3} - \ldots - a_{v-k+1} b_{r+k},$$

siquidem quantitatibus b_m pro indicis m valoribus et minoribus quam k et maioribus quam n, quantatibus autem a_m pro indicis m valoribus et negativis et maioribus quam n valor ipsius 0 tribuitur. Unde posito

$$c_r^{(v)} = \alpha_{r,v}$$

fiunt $\gamma_s^{(v)} = a_{v-s}$, $g_s^{(r)} = -b_{r+s+1}$ pro valoribus 0, 1, 2, 3, ... $k-1$ indicum r et s, et, quia quantitates a_m pro indice m negativo evanescunt, Determinans

$$77.\quad \Sigma \pm \gamma_0^{(0)} \gamma_1' \gamma_2'' \ldots \gamma_{k-1}^{(k-1)} = a_0^k,$$

ideoque a_0^k erit factor superfluus, qui aequationem

$$78.\quad A = \Sigma \pm c_0^{(0)} c_1' c_2'' \ldots c_{n-1}^{(n-1)} = \Sigma \pm \alpha_{0,0} \alpha_{1,1} \alpha_{2,2} \ldots \alpha_{n-1,n-1} = 0$$

afficit, ita ut

$$79.\quad \frac{A}{a_0^k} = 0$$

sit aequatio finalis genuina, quae variabili y eliminata prodit ex aequationibus

$$f(y) = a_0 y^n + a_1 y^{n-1} + a_2 y^{n-2} + \ldots + a_{n-1} y + a_n = 0,$$
$$F(y) = b_k y^{n-k} + b_{k+1} y^{n-k-1} + \ldots \ldots + b_{n-1} y + b_n = 0.$$

Fit autem

$$80.\quad \frac{A}{a_0^k} = \Sigma \pm g_0^{(0)} g_1' g_2'' \ldots g_{n-1}^{(n-1)}$$

siquidem ponitur $g_v^{(r)} = -b_{r+v+1}$ si $v \leqq k-1$ et $g_v^{(r)} = \alpha_{r,v}$ si $v > k-1$, unde patet $\frac{A}{a_0^k}$ esse Determinans, quod provenit ex n aequationibus

$$81.\quad \begin{cases} 0 = -F(y), & 0 = -yF(y), & 0 = -y^2 F(y), & \ldots\ 0 = -y^{k-1} F(y), \\ 0 = m_k, & 0 = m_{k+1}, & 0 = m_{k+2}, & \ldots\ 0 = m_{n-1}, \end{cases}$$

eliminatis n quantitatibus y^{n-1}, y^{n-2}, y^{n-3}, ... y^1, y^0, quarum k primae manifesto adhiberi possunt in locum k aequationum

$$m_0 = 0, \quad m_1 = 0, \quad m_2 = 0, \quad \ldots\ldots, \quad m_{k-1} = 0,$$

quia utrisque simul satisfit; habemus enim

$$m_v = -a_v F(y) - a_{v-1} y F(y) - a_{v-2} y^2 F(y) - \ldots\ldots - a_0 y^v F(y)$$

pro valoribus 0, 1, 2, ... $k-1$ indicis v. Videmus igitur et casu graduum inaequalium aequationum propositarum per eliminationem n quantitatum y^{n-1}, $y^{n-2}, y^{n-3}, \ldots y^1, y^0$ e n aequationibus linearibus perveniri ad ipsam aequationem finalem genuinam factore superfluo non affectam. Sed hae aequationes (81.) non gaudent proprietatibus peculiaribus, quas supra demonstravimus de aequationibus (48.)

$$m_0 = 0, \quad m_1 = 0, \quad m_2 = 0, \quad \ldots\ldots, \quad m_{n-1} = 0,$$

quae ex ipsis (81.) lineariter componuntur, unde melius videtur et hoc casu graduum inaequalium aequationum $f(y) = 0$ et $F(y) = 0$ conservare formam (48.) n aequationum linearium, e quibus n quantitates $y^{n-1}, y^{n-2}, y^{n-3}, \ldots y^1, y^0$ eliminandae sunt. Quo facto aequatio $F(y) = 0$ tanquam consideratur ut aequatio gradus n^{ti}, in qua coëfficientes k potestatum altissimarum ipsi 0 aequalis sint, sive quae k radicibus infinitis gaudeat; atque ubi res hoc modo adepicitur factor a_0^k Determinantis Δ non amplius superfluus est, sed enuntiat, fieri debere $a_0 = 0$, ut aequationes $f(y) = 0$ et $F(y) = 0$ gradus n^{ti} radice communi infinita gaudeant.

Eodem modo, aequatione $F(y) = 0$ gradus $(n-k)^{\text{ti}}$ per y^k multiplicata, erit $y^k F(y) = 0$ aequatio n^{ti} gradus k radicibus ipsi 0 aequalibus gaudens; ac si methodus in paragraphis antecendentibus exposita ad aequationes

$$f(y) = 0 = a_0 y^n + a_1 y^{n-1} + a_2 y^{n-2} + \ldots\ldots + a_{n-1} y + a_n,$$
$$y^k F(y) = 0 = b_k y^n + b_{k+1} y^{n-1} + b_{k+2} y^{n-2} + \ldots\ldots + b_n y^k$$

adhibetur, eadem ratione demonstratur Determinans aequationum (48.)

$$m_0 = 0, \quad m_1 = 0, \quad m_2 = 0, \quad \ldots\ldots \quad m_{n-1} = 0$$

gaudere factore a_n^k, qui ipsi 0 aequalis positus exprimit conditionem, cui satisfieri debet, ut aequatio $f(y) = 0$ radice $y = 0$ cum aequatione $y^k F(y) = 0$ communi gaudeat. Siquidem in formulis paragraphi antecedentis loco b_m ponitur b_{k+m}, et $b_{k+m} = 0$ pro indicis m valoribus et negativis et maioribus quam $n-k$. Ubi igitur divisio per factorem a_n^k instituitur, Determinans illud ipsi 0 aequale positum, praebebit aequationem finalem genuinam, quae ex aequationibus $f(y) = 0$ $F(y) = 0$ prodit variabili y eliminata; atque erit haec aquatio Determinans, quod ex aequationibus

$$82. \quad \begin{cases} m_0 = 0, \quad m_1 = 0, \quad m_2 = 0, \quad \ldots\ldots \quad m_{n-k-1} = 0, \\ y^{k-1} F(y) = 0, \quad y^{k-2} F(y) = 0, \quad \ldots\ldots \quad F(y) = 0 \end{cases}$$

provenit, eliminatis n quantitatibus $y^{n-1}, y^{n-2}, y^{n-3}, \ldots\ldots y^0$. Quarum aequa-

tionum k ultimae locum tenent ipsarum

$$m_{n-k} = 0, \quad m_{n-k+1} = 0, \quad m_{n-k+2} = 0, \quad \dots\dots \quad m_{n-1} = 0.$$

Fit enim pro k valoribus $n-k$, $n-k+1$, $n-k+2$, ... $n-1$ indicis v

$$m_v = a_{v+1}y^{k-1}F(y) + a_{v+2}y^{k-2}F(y) + a_{v+3}y^{k-3}F(y) + \dots\dots + a_n y^{v-(n-k)}F(y)$$

ex aequatione (65.)

Aequationibus (47.) et casu graduum inaequalium etiam aequationibus (81.) et (82.) clarissime ante oculos ponitur, hanc clarissimi *Bézout* Methodum eliminationis eandem esse cum Methodo, quam a clarissimo *Sylvester* in diario „The London and Edinburgh philosophical magazine and journal of science" propositam esse, clarissimus *Richelot* commemorat in commentatione „Nota ad theoriam eliminationis pertinens" Diarii Crell. tom. XXI. inserta. Hac enim problema eliminationis variabilis y ex aequationibus

$$f(y) = a_0 y^n + a_1 y^{n-1} + a_2 y^{n-2} + \dots\dots + a_n = 0,$$
$$F(y) = b_k y^{n-k} + b_{k+1} y^{n-k-1} + b_{k+2} y^{n-k-2} + \dots\dots + b_n = 0$$

revocatur ad eliminationem $(2n-k)$ quantitatum y^{2n-k-1}, y^{2n-k-2}, y^{2n-k-3}, ... y^1, y^0 e systemate $2n-k$ aequationum linearium

$$83. \begin{cases} f(y) = 0, \quad yf(y) = 0, \quad y^2 f(y) = 0, \quad \dots\dots \quad y^{n-k-1}f(y) = 0, \\ F(y) = 0, \quad yF(y) = 0, \quad y^2 F(y) = 0, \quad \dots\dots \quad y^{n-1}F(y) = 0; \end{cases}$$

unde ipso intuitu systematis n aequationum linearium (47.)

$$m_0 = 0, \quad m_1 = 0, \quad m_2 = 0, \quad \dots\dots \quad m_{n-1} = 0$$

(sive etiam ipsarum (81.)) inter n quantitates y^{n-1}, y^{n-2}, ... y^1, y^0 elucet, methodum clarissimi *Bézout* omnino eandem esse, sed perfectiorem, quippe quae doceat, quomodo algorithmo elegantissimo eliminatio $n-k$ quantitatum y^n, y^{n+1}, y^{n+2}, ... y^{2n-k-1} semper perfici possit, ita ut $2n-k$ aequationes (83.) inter $2n-k$ quantitates redeant in systema n aequationum (47.) aut (81.) inter $n-1$ quantitates y^{n-1}, y^{n-2}, ... y^1, y^0.

8.

Alia eliminationis methodus a cl. *Eulero* in veteribus Commentariis Academiae Berolinensis T. N. ad a. 1748 proposita, quae in libris de elementis matheseos conscriptis pro casu aequationum radicibus explicitis gaudentium doceri solet, eo continetur, quod propositis aequationibus

$$84. \begin{cases} f(y) = 0 = a_0 y^n + a_1 y^{n-1} + \dots\dots + a_{n-1}y + a_n = a_0(y-y_1)(y-y_2)\dots\dots(y-y_n), \\ F(y) = 0 = b_k y^{n-k} + b_{k+1} y^{n-k-1} + \dots\dots + b_{n-1}y + b_n = b_k(y-\eta_1)(y-\eta_2)\dots\dots(y-\eta_{n-k}), \end{cases}$$

radix y_1 aequationis alterius $f(y) = 0$, quam cum altera $F(y) = 0$ communem

habet, in hanc substituatur; quo facto inter coëfficientes a_m et b_m prodeat aequatio

$$85. \quad F(y_1) = 0,$$

respectis coëfficientibus a_m irrationalis; qua rationali reddita et denominatoribus per multiplicationem sublatis, inveniatur aequatio finalis genuina quaesita. Aequatio autem irrationalis $F(y_1) = 0$ rationalis redditur multiplicatione facta per $F(y_2)F(y_3)F(y_4)\ldots F(y_n)$; constabit enim productum

$$86. \quad F(y_1)F(y_2)F(y_3)\ldots F(y_n) = 0$$

terminis

$$M\Sigma y_1^{m_1} y_2^{m_2} y_3^{m_3} \ldots\ldots y_\mu^{m_\mu},$$

in quibus M designat productum e coëfficientibus b_m conflatum dimensionis n^{tae}, $\Sigma y_1^{m_1} y_2^{m_2} y_3^{m_3} \ldots y_\mu^{m_\mu}$ functionem symmetricam radicum $y_1, y_2, y_3, \ldots y_n$ aequationis $f(y) = 0$, quae e termino $y_1^{m_1} y_2^{m_2} y_3^{m_3} \ldots y_\mu^{m_\mu}$ originem ducit. Hanc vero constat esse functionem rationalem coëfficientium a_m, numeratore dimensionis m_1^{tae} et denominatore $a_0^{m_1}$ gaudentem, siquidem m_1 maximus est e numeris integris positivis $m_1, m_2, m_3, \ldots m_\mu$. Qui quum numerum $n-k$ superare nequeant, a_0^{n-k} generaliter minima erit potestas ipsius a_0, per quam multiplicata pars sinistra aequationis (86.) fiat functio integra coëfficientium a_m et b_m, harum dimensionis n^{tae} illarum dimensionis $(n-k)^{\text{tae}}$. Unde generaliter erit

$$87. \quad a_0^{n-k} F(y_1) F(y_2) F(y_3) \ldots F(y_n) = 0$$

aequatio finalis genuina quaesita, factore superfluo non affecta.

In terminis autem aequationis (86.) forma $M\Sigma y_1^{n-k} y_2^{m_2} y_3^{m_3} \ldots y_n^{m_n}$ productum M e coëfficientibus b_m conflatum manifesto continebit factorem b_{n-k}. Si igitur aequationes $f(y) = 0$ et $F(y) = 0$ forte ita comparatae sunt, ut fiat $b_k = a_0$, denominatores ex aequatione (86.) exterminantur, ubi multiplicatio instituitur per a_0^{n-k-1}; ac si quantitates a_m et b_m polynomia ipsius x sunt et c designat polynomium ipsius x gradus altissimi, quod polynomia a_0 et b_k simul metitur, erit

$$88. \quad a^{n-k-1} \frac{a_0}{c} F(y_1) F(y_2) F(y_3) \ldots F(y_n) = 0$$

functio rationalis integra ipsius x; aequatio autem $c = 0$ eos praebebit valores ipsius x, pro quibus aequationes $f(y) = 0$, $F(y) = 0$ habeant unam radicem communem *infinitam*.

Ubi eliminatio ipsius y secundum methodum *Bézoutianam* ex aequationibus

$$f(y) = a_0 y^n + a_1 y^{n-1} + a_2 y^{n-2} + \dots + a_n = 0,$$
$$y^k F(y) = b_k y^n + b_{k+1} y^{n-1} + b_{k+2} y^{n-2} + \dots + b_n y^k = 0$$

instituitur, erit si a_0 et b_k factore maximo communi c gaudent, e numero aequationum linearium

$$m_0 = 0, \quad m_1 = 0, \quad m_2 = 0, \quad \dots \quad m_{n-k-1} = 0,$$
$$F(y) = 0, \; yF(y) = 0, \; y^2 F(y) = 0, \; \dots \; y^{k-1} F(y) = 0,$$

e quibus quantitates y^{n-1}, y^{n-2}, y^{n-3}, ... y^1, y^0 eliminandae sunt, ipsa

$$m_0 = a_0 y^k F(y) - b_k f(y) = 0$$

per c divisibilis; unde factor c metietur aequationem finalem, ad quam eliminatione facta pervenitur; quo per divisionem sublato prodibit aequatio (88.) conditionem *unius* radicis communis *infiniti* aequationum $f(y) = 0$ et $F(y) = 0$ non continens. Quoties autem $a_0 = b_k$ ad aequationem (88.), quae hoc casu in formam

$$a_0^{n-k-1} F(y_1) F(y_2) F(y_3) \dots F(y_n) = 0$$

abit, per methodum *Bézoutianam* simplicius pervenitur, ubi ab initio haec methodus adhibetur ad aequationes gradus $(n-1)^{ti}$

$$\frac{m_0}{a_0} = y^k F(y) - f(y) = 0 = (b_{k+1} - a_1) y^{n-1} + (b_{k+2} - a_2) y^{n-2} + \dots$$
$$\dots + (b_n - a_{n-k}) y^k - a_{n-k+1} y^{k-1} - a_{n-k+2} y^{k-2} - \dots - a_n,$$
$$y^{k-1} F(y) = b_k y^{n-1} + b_{k+1} y^{n-2} + b_{k+2} y^{n-3} + \dots + b_n y^{k-1} = 0,$$

quarum coëfficientes ex ipsis b_m et a_m lineariter pendent; et quarum aequatio finalis a factore $a_0 = b_k$ libera erit, qui ipsi 0 aequalis positus exprimit conditionem *unius* radicis communis *infiniti* aequationum $f(y) = 0$, $F(y) = 0$.

9.

Notum est e theoria aequationum algebraicarum, radicem, quam aequatio $\varphi(x,y) = 0 = p_0 y^n + p_1 y^{n-1} + p_2 y^{n-2} + \dots + p_n = p_0 (y - y_1)(y - y_2) \dots (y - y_n)$ cum aequatione

$$\varphi'(y) = 0 = n p y^{n-1} + (n-1) p_1 y^{n-2} + (n-2) p_2 y^{n-3} + \dots + p_{n-1}$$

communem habeat, m^{ies} inveniri in numero radicum aequationis $\varphi(x, y) = 0$, si in numero radicum aequationis $\varphi'(y) = 0$ $(m-1)^{ies}$ inveniatur. Excepto casu, quo radix communis aequationum $\varphi(x, y) = 0$, $\varphi'(y) = 0$ infinita est. Tum enim radix illa toties in numero radicum aequationis $\varphi(x, y)$ invenietur, quoties in numero radicum aequationis $\varphi'(y) = 0$ inest; ut enim $\varphi'(y) = 0$ gaudeat $m - 1$ radicibus infinite magnis, fieri debent $p_0 = 0$, $p_1 = 0$, $p_2 = 0$, ... $p_{m-2} = 0$; quo facto etiam $\varphi(x, y) = 0$ non nisi $m - 1$ radicibus infinite magnis gaudebit.

Unde secundum ea, quae in paragrapho antecedenti exposita sunt, patet, aequationem

$$89.\quad p_0^{n-2}\varphi'(y_1)\varphi'(y_2)\varphi'(y_3)\dots\varphi'(y_n) = 0,$$

cuius pars sinistra coëfficientium p_m functio rationalis integra est dimensionis $(2n-2)^{\text{tae}}$, continere conditionem, cui coëfficientes p_m obnoxiae esse debeant, ut radix y aequationibus $\varphi(x,y)=0$ et $\varphi'(y)=0$ communis inter radices aequationis $\varphi(x,y)=0$ saltem bis inveniatur, sive ut aequatio $\varphi(x,y)=0$ radicibus gaudeat aequalibus. Factor enim p_0, qui ipsi 0 aequalis positus exprimit conditionem radicis communis infinitae aequationum $\varphi(x,y)=0$, $\varphi'(y)=0$, quae tamen in numero radicum aequationis $\varphi(x,y)=0$ *semel* tantum invenitur, in aequatione (89.) non amplius inest.

Eadem aequatio (89.) inveniri debet, si methodus *Bézoutiana* adhibetur ad aequationes

$$\varphi'(y)=0=np_0y^{n-1}+(n-1)p_1y^{n-2}+(n-2)p_2y^{n-3}+\dots+p_{n-1},$$
$$n\varphi(x,y)-y\varphi'(y)=0=p_1y^{n-1}+2p_2y^{n-2}+3p_3y^{n-3}+\dots+np_n.$$

In formulis igitur de hac methodo supra propositis ponendum erit

$$a_0=0,\ a_1=np_0,\ a_2=(n-1)p_1,\ a_3=(n-2)p_2,\ \dots\ a_n=p_{n-1},$$
$$b_0=0,\ b_1=p_1,\quad b_2=2p_2,\qquad b_3=3p_3,\ \dots\dots\ b_n=np_n$$

generaliter pro valoribus 0, 1, 2, 3, ... $n-1$ indicis m

$$a_{m+1} = (n-m)p_m,\quad b_{m+1} = (m+1)p_{m+1}.$$

Quo facto fiunt $m_0=0$ et pro valoribus 1, 2, 3, ... $n-1$ indicis v, $\alpha_{n,v}=0$, atque aequatio quaesita obtinetur, eliminatis $n-1$ quantitatibus y^{n-2}, y^{n-3}, ... y^1, y^0 ex $n-1$ aequationibus linearibus

$$0 = \alpha_{1,1}y^{n-2}+\alpha_{2,1}y^{n-3}+\alpha_{3,1}y^{n-4}+\dots+\alpha_{n-1,1}y^0,$$
$$0 = \alpha_{1,2}y^{n-2}+\alpha_{2,2}y^{n-3}+\alpha_{3,2}y^{n-4}+\dots+\alpha_{n-1,2}y^0,$$
$$0 = \alpha_{1,3}y^{n-2}+\alpha_{2,3}y^{n-3}+\alpha_{3,3}y^{n-4}+\dots+\alpha_{n-1,3}y^0,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$0 = \alpha_{1,n-1}y^{n-2}+\alpha_{2,n-1}y^{n-3}+\alpha_{3,n-1}y^{n-4}+\dots+\alpha_{n-1,n-1}y^0,$$

et fiunt, quum propter $a_0=0$, $b_0=0$ pro valoribus 1, 2, 3, ... $n-1$ indicum r et v aequationibus (50.) prodeant

$$\begin{aligned}\alpha_{r,v} = \alpha_{v,r} &= a_{v+1}b_r+a_{v+2}b_{r-1}+a_{v+3}b_{r-3}+\dots+a_{v+r-1}b_1\\ &\quad -b_{v+1}a_r-b_{v+2}a_{r-1}-b_{v+3}a_{r-3}-\dots-b_{v+r-1}a_1\\ &= a_{r+1}b_v+a_{r+2}b_{v-1}+a_{r+3}b_{v-3}+\dots+a_{r+v-1}b_1\\ &\quad -b_{r+1}a_v-b_{r+2}a_{v-1}-b_{r+3}a_{v-3}-\dots-b_{r+v-1}a_1,\end{aligned}$$

substitutis valoribus $a_{v+1}=(n-v)p_v$, $b_r=rp_r$,

$$\begin{aligned}\alpha_{r,v} = \alpha_{v,r} &= (n-v)rp_rp_v + (n-v-1)(r-1)p_{r-1}p_{v+1} \\ &+ (n-v-2)(r-2)p_{r-2}p_{v+2} + \dots + (n-v-r+1)p_1p_{v+r-1} \\ &- (n-r+1)(v+1)p_{r-1}p_{v+1} - (n-r+2)(v+2)p_{r-2}p_{v+2} \\ &- (n-r+3)(v+3)p_{r-3}p_{v+3} - \dots - n(v+r)p_0p_{v+r} \\ &= (n-r)vp_vp_r + (n-r-1)(v-1)p_{v-1}p_{r+1} \\ &+ (n-r-2)(v-2)p_{v-2}p_{r+2} + \dots + (n-r-v+1)p_1p_{r+v-1} \\ &- (n-v+1)(r+1)p_{r-1}p_{v+1} - (n-v-2)(r+2)p_{v-2}p_{r+2} \\ &- (n-v+3)(r+3)p_{r-3}p_{v+3} - \dots - n(r+v)p_0p_{r+v}.\end{aligned}$$

Supra vero invenimus

$$\begin{aligned}I_{r,v} = I_{v,r} &= \frac{n-v}{n}rp_rp_v - \overset{r}{\underset{0}{\Sigma_m}}(v-r+2m)p_{r-m}p_{v+m} \\ &= \frac{n-r}{n}vp_vp_r - \overset{v}{\underset{0}{\Sigma_m}}(r-v+2m)p_{v-m}p_{r+m}\end{aligned}$$

unde patet esse

$$\alpha_{r,v} = nI_{r,v},$$

ideoque fieri, signo determinantis apte determinato:

90. $n^{n-1}L = n^{n-1}\Sigma \pm I_{1,1}I_{2,2}I_{3,3}\dots I_{n-1,n-1} = p_0^{n-2}\varphi'(y_1)\varphi'(y_2)\varphi'(y_3)\dots\varphi'(y_n)$,

sive aequationum $L=0$ eam exprimere conditionem, cui coëfficientes p_m aequationis $\varphi(x,y)=0$ obnoxiae esse debeant, ut haec aequatio radicibus aequalibus gaudeat, q. d. e.

10.

Ubi formulae ceterae, e methodo eliminationis ***Bézoutiana*** profluentes, quas supra e commentatione clarissimi ***Jacobi*** petiimus, ad aequationes $\varphi'(y)=0$, $n\varphi(x,y)-y\varphi'(y)=0$ adhibentur, formulas praebent elegantissimas, quibus expressio

$$3.\quad \frac{Q_2y^{n-2}+Q_3y^{n-3}+Q_4y^{n-4}+\dots+Q_n}{\varphi'(y)},$$

quam ut formam functionis algebraicae integrandae praestantissimam proponimus, ad alteram revocatur, respectu ipsius y integram,

$$2.\quad M_1y^{n-1}+M_2y^{n-2}+M_3y^{n-3}+\dots+M_{n-1}y+M_n,$$

in quam functionem integrandam algebraicam redactam esse geometrae supponere solent. Siquidem, ut supra, $Q_2, Q_3, Q_4, \dots Q_n, M_1, M_2, M_3, \dots M_n$ designant functiones rationales ipsius x; y autem radicem aequationis irreductibilis $\varphi(x,y)=0$.

Positis enim $a_0=0$, $b_0=0$, $a_m=(n-m+1)p_{m-1}$, $b_m=mp_m$ fiunt in formulis paragraphi 6[ti]

$$m_0 = 0, \quad \alpha_{r,0} = \alpha_{0,r}, \quad A_0 = 0, \quad A_1 = 0, \quad \alpha_{r,v} = n I_{r,v}, \quad A = n^{n-1} L$$

atque

$$91. \begin{cases} m_v = \{p_1 y^{v-1} + 2 p_2 y^{v-2} + 3 p_3 y^{v-3} + \dots + v p_v\} \varphi'(y) \\ \quad - \{n p_0 y^{v-1} + (n-1) p_1 y^{v-2} + (n-2) p_2 y^{v-3} + \dots + p_{v-1}\} \{n \varphi(x,y) - y \varphi'(y)\} \\ \quad = \{n \{I_{1,v} y^{n-2} + I_{2,v} y^{n-3} + I_{3,v} y^{n-4} + \dots + I_{n-1,v} y^0\}, \end{cases}$$

$$92. \quad n L y^{n-1-r} = A_{r+1} m_1 + A_{r+2} m_2 + A_{r+3} m_3 + \dots + A_{r+n-1} m_{n-1}$$

pro omnibus indicum r et v valoribus 1, 2, 3, ... $n-1$; siquidem hoc loco per $n^{n-2} A_{r+v}$ repraesentamus, quod supra per A_{r+v} designabatur.

Quoties igitur y est radix aequationis $\varphi(x, y) = 0$, fit ex aequatione (91.)

$$m_v = n \varphi'(y) \{p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \dots + p_{v-1} y + \tfrac{v}{n} p_v\},$$

sive

$$p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \dots + p_{v-1} y + \frac{v}{n} p_v = \frac{I_{1,v} y^{n-2} + I_{2,v} y^{n-3} + \dots + I_{n-1,v}}{\varphi'(y)},$$

ideoque ex aequatione (92.)

$$93. \quad \frac{y^{n-1-r}}{\varphi'(y)} = \frac{1}{L} \sum_1^{n-1} A_{r+v} \left(p_0 y^v + p_1 y^{v-1} + p_2 y^{v-2} + \dots + p_{v-1} y + \frac{v}{n} p_v\right).$$

Quo valore ipsius $\frac{y^{n-1-r}}{\varphi'(y)}$ in expressionem (3.) substituto, prodit, posito

$$94. \quad A_{r+1} Q_1 + A_{r+2} Q_2 + A_{r+3} Q_3 + \dots + A_{r+n-1} Q_{n-1} = L T_r,$$

$$95. \quad \frac{\sum_1^{n-1} Q_{n-r} y^{n-r-1}}{\varphi'(y)} = \sum_1^{n-1} T_r \left(p_0 y^r + p_1 y^{r-1} + p_2 y^{r-2} + \dots + p_{r-1} y + \frac{r}{n} p_r\right)$$
$$= M_1 y^{n-2} + M_2 y^{n-3} + M_3 y^{n-4} + \dots + M_{n-2} y + M_{n-1}$$

et fiunt pro indicis r valoribus 1, 2, 3, ... $n-1$,

$$M_r = p_0 T_{n-r} + p_1 T_{n-r+1} + p_2 T_{n-r+2} + \dots + p_{r-1} T_{n-1},$$

$$n M_n = -\sum_1^n (M_1 y^{n-1} + M_2 y^{n-2} + \dots + M_{n-1} y)$$
$$= p_1 T_1 + 2 p_2 T_2 + 3 p_3 T_3 + \dots + (n-1) p_{n-1} T_{n-1}.$$

Unde formae (2.) et (3.) altera ad alteram reducuntur per resolutionem systematis $n-1$ aequationum linearium inter $n-1$ incognitas. Nam e forma (3.) ad formam (2.) pervenire resolvendum erit systema $n-1$ aequationum linearium

$$96. \begin{cases} Q_1 = l_{1,1} T_1 + l_{2,1} T_2 + l_{3,1} T_3 + \dots + l_{n-1,1} T_{n-1}, \\ Q_2 = l_{1,2} T_1 + l_{2,2} T_2 + l_{3,2} T_3 + \dots + l_{n-1,2} T_{n-1}, \\ Q_3 = l_{1,3} T_1 + l_{2,3} T_2 + l_{3,3} T_3 + \dots + l_{n-1,3} T_{n-1}, \\ \dots \\ Q_{n-1} = l_{1,n-1} T_1 + l_{2,n-1} T_2 + l_{3,n-1} T_3 + \dots + l_{n-1,n-1} T_{n-1}. \end{cases}$$

Quibus resolutis per aequationes

$$97.\quad \begin{cases} LT_1 = A_2Q_2 + A_3Q_3 + A_4Q_4 + \dots + A_nQ_n, \\ LT_2 = A_3Q_2 + A_4Q_3 + A_5Q_4 + \dots + A_{n+1}Q_n, \\ LT_3 = A_4Q_2 + A_5Q_3 + A_6Q_4 + \dots + A_{n+2}Q_n, \\ \dots\dots\dots\dots\dots\dots\dots \\ LT_{n-1} = A_nQ_n + A_{n+1}Q_3 + A_{n+2}Q_4 + \dots + A_{2n-2}Q_n \end{cases}$$

exhibentur coëfficientes M_1, M_2, M_3, ... M_{n-1} per formulas

$$98.\quad \begin{cases} M_1 = p_0T_{n-1}, \\ M_2 = p_1T_{n-1} + p_0T_{n-2}, \\ M_3 = p_2T_{n-1} + p_1T_{n-2} + p_0T_{n-3}, \\ \dots\dots\dots\dots\dots\dots \\ M_{n-1} = p_{n-2}T_{n-1} + p_{n-3}T_{n-2} + p_{n-4}T_{n-3} + \dots + p_0T_1, \end{cases}$$

et M_n per aequationem

$$99.\quad nM_n = -\sum_1^n {}_i(M_1y_i^{n-1} + M_2y_i^{n-2} + \dots + M_{n-1}y_i)$$
$$= p_1T_1 + 2p_2T_2 + 3p_3T_3 + \dots + (n-1)p_{n-1}T_{n-1}.$$

Contra ut forma (2.) functionis algebraicae integrandae

$$M_1y^{n-1} + M_2y^{n-2} + \dots + M_{n-1}y + M_n,$$

in qua

$$nM_n = -\sum_1^n {}_i(M_1y_i^{n-1} + M_2y_i^{n-2} + \dots + M_{n-1}y_i),$$

redigatur in formam (3.), ponendum erit

$$M_1y^{n-1} + M_2y^{n-2} + \dots + M_{n-1}y = \sum_1^{n-1} {}_\upsilon T_\upsilon(p_0y^\upsilon + p_1y^{\upsilon-1} + \dots + p_{\upsilon-1}y),$$

ideoque $\quad nM_n = p_1T_1 + 2p_2T_2 + 3p_3T_3 + \dots + (n-1)p_{n-1}T_{n-1}.$

Quo facto exprimuntur $n-1$ quantitates T_1, T_2, ... T_{n-1} per datas M_1, M_2, M_3, ... M_{n-1}, ope systematis (98.) $n-1$ aequationum linearium. Quibus resolutis ipsae aequationes (96.) praebent valores quaesitos coëfficientium Q_2, Q_3, ... Q_n formae (3.). Adnotandum est, ope aequationum, quibus quantitates A_υ obnoxias esse, supra ostendimus

$$\left.\begin{array}{l} p_1A_2 + 2p_2A_3 + 3p_3A_4 + \dots + np_nA_{n+1} = 0, \\ p_1A_3 + 2p_2A_4 + 3p_3A_5 + \dots + np_nA_{n+2} = 0, \\ p_1A_4 + 2p_2A_5 + 3p_3A_6 + \dots + np_nA_{n+3} = 0, \\ \dots\dots\dots\dots\dots\dots\dots \\ p_1A_{n-1} + 2p_2A_n + 3p_3A_{n+1} + \dots + np_nA_{2n-2} = 0, \end{array}\right\}$$

$$\begin{cases} np_0A_2 + (n-1)p_1A_3 + (n-2)p_2A_4 + \dots + p_{n-1}A_{n+1} = 0, \\ np_0A_3 + (n-1)p_1A_4 + (n-2)p_2A_5 + \dots + p_{n-1}A_{n+2} = 0, \\ np_0A_4 + (n-1)p_1A_5 + (n-2)p_2A_6 + \dots + p_{n-1}A_{n+3} = 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ np_0A_{n-1} + (n-1)p_1A_n + (n-2)p_2A_{n+1} + \dots + p_{n-1}A_{2n-2} = 0 \end{cases}$$

e quibus etiam sequuntur

$$p_0 A_2 + p_1 A_3 + p_2 A_4 + \ldots + p_n A_{n+2} = 0,$$
$$p_0 A_3 + p_1 A_4 + p_2 A_5 + \ldots + p_n A_{n+3} = 0,$$
$$p_0 A_4 + p_1 A_5 + p_2 A_6 + \ldots + p_n A_{n+4} = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$p_0 A_{n-2} + p_1 A_{n-1} + p_2 A_n + \ldots + p_n A_{2n-2} = 0,$$

coëfficientes M_1, M_2, M_3, ... M_{n-1} (valoribus ipsarum T_1, T_2, ... T_{n-1} in aequationes (98.) substitutis), sub variis formis repraesentari posse ut functiones coëfficientium Q_2, Q_3, ... Q_n.

(Cont. seq.)

22.

Note sur la convergence de la série de Taylor.

(Par Mr. *P. Tchebicheff* à Moscou.)

D'après la règle de Mr. *Cauchy* la série

$$fa+\frac{z}{1}f'a+\frac{z^2}{1.2}f''a+\frac{z^3}{1.2.3}f'''a+\ldots.+\frac{z^{n-1}}{1.2.3\ldots.(n-1)}f^{(n-1)}a$$
$$+\frac{z^n}{1.2.3\ldots.(n-1)n}f^{(n)}a+\ldots$$

sera convergente toutes les fois que

$$\lim.\left[\text{mod.}\frac{z^n}{1.2.3\ldots.n}f^{(n)}a\right]^{\frac{1}{n}}_{n=\infty}<1,$$

ou, ce qui est le même,

$$1.\quad \lim.\left[(\text{mod.}z)^n.\ \text{mod.}\frac{f^{(n)}a}{1.2.3\ldots.n}\right]^{\frac{1}{n}}_{n=\infty}<1,$$

et divergente, si

$$2.\quad \lim.\left[\text{mod.}\frac{z^n}{1.2.3\ldots.n}f^{(n)}a\right]^{\frac{1}{n}}_{n=\infty}>1.$$

Mais on a

$$fa=\frac{1}{2\pi}\int_{-\pi}^{+\pi}f(a+Re^{p\sqrt{-1}})dp,$$

lorsque la fonction $f(a+re^{p\sqrt{-1}})$ est finie et continue, quel que soit p, pour $r=R$ ou pour une valeur quelconque de r plus petite que R *), et de même

$$3.\quad f'a=\frac{1}{2\pi}\int_{-\pi}^{+\pi}f'(a+Re^{p\sqrt{-1}})dp,$$

$$4.\quad f''a=\frac{1}{2\pi}\int_{-\pi}^{+\pi}f''(a+Re^{p\sqrt{-1}})dp,$$

. . . .

$$5.\quad f^{(n-1)}a=\frac{1}{2\pi}\int_{-\pi}^{+\pi}f^{(n-1)}(a+Re^{p\sqrt{-1}})dp,$$

$$6.\quad f^{(n)}a=\frac{1}{2\pi}\int_{-\pi}^{+\pi}f^{(n)}(a+Re^{p\sqrt{-1}})dp,$$

. . . .

---

*) *Cauchy,* Exercices d'Analyse et de Physique Mathématique tome I. page 356.

si $f'(a+Re^{p\sqrt{-1}})$, $f''(a+Re^{p\sqrt{-1}})$, ... $f^{(n-1)}(a+Re^{p\sqrt{-1}})$, $f^{(n)}(a+Re^{p\sqrt{-1}})$ sont aussi finies et continues, quel que soit p, pour toutes les valeurs r qui ne surpassent pas R.

Or l'intégration par parties donne

$$\int_{-\pi}^{+\pi} f'(a+Re^{p\sqrt{-1}})dp = \frac{1}{R}\int_{-\pi}^{+\pi} e^{-p\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

$$\int_{-\pi}^{+\pi} f''(a+Re^{p\sqrt{-1}})dp = \frac{1.2}{R^2}\int_{-\pi}^{+\pi} e^{-2p\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

. . . .

$$\int_{-\pi}^{+\pi} f^{(n-1)}(a+Re^{p\sqrt{-1}})dp = \frac{1.2.3\ldots.(n-1)}{R^{n-1}}\int_{-\pi}^{+\pi} e^{-(n-1)p\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

$$\int_{-\pi}^{+\pi} f^{(n)}(a+Re^{p\sqrt{-1}})dp = \frac{1.2.3\ldots.(n-1)n}{R^{n}}\int_{-\pi}^{+\pi} e^{-np\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

. . . .

ce qui change les équations (3, 4, 5 et 6) en celles-ci

$$7.\quad f'a = \frac{1}{2\pi}\cdot\frac{1}{R}\int_{-\pi}^{-\pi} e^{-p\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

$$8.\quad f''a = \frac{1}{2\pi}\cdot\frac{1.2}{R^2}\int_{-\pi}^{+\pi} e^{-2p\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

. . . .

$$9.\quad f^{(n-1)}a = \frac{1}{2\pi}\cdot\frac{1.2.3\ldots.(n-1)}{R^{n-1}}\int_{-\pi}^{+\pi} e^{-(n-1)p\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

$$10.\quad f^{(n)}a = \frac{1}{2\pi}\cdot\frac{1.2.3\ldots.(n-1)n}{R^{n}}\int_{-\pi}^{+\pi} e^{-np\sqrt{-1}}f(a+Re^{p\sqrt{-1}})dp,$$

. . . .

Désignant par λ la plus grande valeur du module de l'expression $f(a+Re^{p\sqrt{-1}})$ pour toutes les valeurs de p, nous trouverons que les modules mod. $[e^{-p\sqrt{-1}}f(a-Re^{p\sqrt{-1}})]$, mod. $[e^{-2p\sqrt{-1}}f(a+Re^{p\sqrt{-1}})]$, ... mod. $[e^{-(n-1)p\sqrt{-1}}f(a-Re^{p\sqrt{-1}})]$, mod. $[e^{-np\sqrt{-1}}f(a+Re^{p\sqrt{-1}})]$ ne surpassent pas λ; car les modules des expressions $e^{-p\sqrt{-1}}$, $e^{-2p\sqrt{-1}}$, ... $e^{-(n-1)p\sqrt{-1}}$, $e^{-np\sqrt{-1}}$ sont égaux à l'unité.

Cela étant, on conclut des équations (7, 8, 9 et 10)

$$\text{mod.}\,\frac{f'a}{2} < \frac{1}{2\pi}\cdot\frac{1}{R}\cdot\lambda\int_{-\pi}^{-\pi}dp < \frac{\lambda}{R};$$

$$\text{mod.}\,\frac{f''a}{1.2} < \frac{1}{2\pi}\cdot\frac{1}{R^2}\cdot\lambda\int_{-\pi}^{-\pi}dp < \frac{\lambda}{R^2};$$

. . . .

$$\text{mod.}\frac{f^{(n-1)}a}{1.2.3\ldots.(n-1)} < \frac{1}{2\pi}\cdot\frac{1}{R^{(n-1)}}\cdot\lambda\int_{-\pi}^{+\pi}dp < \frac{\lambda}{R^{(n-1)}};$$

$$\text{mod.}\frac{f^{(n)}a}{1.2.3\ldots.(n-1)n} < \frac{1}{2\pi}\cdot\frac{1}{R^n}\cdot\lambda\int_{-\pi}^{+\pi}dp < \frac{\lambda}{R^n}.$$

D'après cela la condition (1.) de la convergence de la série

$$fa+\frac{z}{1}f'a+\frac{z^2}{1.2}f''a+\frac{z^3}{1.2.3}f'''a+\ldots.+\frac{z^{n-1}}{1.2.3\ldots.(n-1)}f^{(n-1)}a$$
$$+\frac{z^n}{1.2.3\ldots.(n-1)n}f^{(n)}a+\ldots.$$

se réduit à celle-ci:

$$\lim.\left[\frac{(\text{mod.}z)^n\lambda}{R^n}\right]_{n=\infty}^{\frac{1}{n}} < 1;$$

ou simplement à

$$\text{mod.}z < R,$$

la limite de $\lambda^{\frac{1}{n}}$ pour $n=\infty$ étant l'unité. Donc la série de *Taylor*

$$11.\quad fa+\frac{z}{1}f'a+\frac{z^2}{1.2}f''a+\frac{z^3}{1.2.3}f'''a+\ldots.+\frac{z^{n-1}}{1.2.3\ldots.(n-1)}f^{(n-1)}a$$
$$+\frac{z^n}{1.2.3\ldots.(n-1)n}f^{(n)}a+\ldots.$$

sera convergente si le module de z est plus petit que R, où, comme nous l'avons dit, les expressions

$f(a+re^{p\sqrt{-1}})$, $f'(a+re^{p\sqrt{-1}})$, ... $f^{(n-1)}(a+re^{p\sqrt{-1}})$, $f^{(n)}(a+re^{p\sqrt{-1}})$, ...
restent finies et continues, quel que soit p, pour $r=R$ ou pour une valeur quelconque de $r<R$. En d'autres termes: La série de *Taylor*

$$fa+\frac{z}{1}f'a+\frac{z^2}{1.2}f''a+\frac{z^3}{1.2.3}f'''a+\ldots.+\frac{z^{n-1}}{1.2.3\ldots.(n-1)}f^{(n-1)}a$$
$$+\frac{z^n}{1.2.3\ldots.(n-1)n}f^{(n)}a+\ldots.$$

sera convergente si le module de z est au dessous du module de la valeur imaginaire de x qui rend infinie ou discontinue au moins une des fonctions

$f(a+x)$, $f'(a+x)$, $f''(a+x)$, ... $f^{(n-1)}(a+x)$, $f^{(n)}(a+x)$, ...

Mais ces conditions toutes, sont-elles nécessaires pour la convergence de la série de *Taylor*? C'est-à-dire: la série de *Taylor* (11.) est-elle toujours divergente pour une valeur de z, dont le module est plus grand que celui de la valeur de x qui rend au moins une des fonctions

$f(a+x)$, $f'(a+x)$, $f''(a+x)$, ... $f^{(n-1)}(a+x)$, $f^{(n)}(a+x)$....
infinie ou discontinue? Voilà ce que nous allons examiner.

Si la fonction $f^{(m)}(a+x)$, par exemple, devient infinie ou discontinue pour $x=X$, au moins une des séries

$$f^{(m)}(a+X) = f^{(m)}\,a+\frac{X}{1}f^{(m+1)}a+\frac{X^2}{1.2}f^{(m+2)}a+\dots$$
$$\dots+\frac{X^{n-m-1}}{1.2.3\dots(n-m-1)}f^{(n-1)}a+\frac{X^{n-m}}{1.2.3\dots(n-m-1)(n-m)}f^{(n)}a+\dots,$$
$$f^{(m+1)}(a+X) = f^{(m+1)}a+\frac{X}{1}f^{(m+2)}a+\frac{X^2}{1.2}f^{(m+3)}a+\dots$$
$$\dots+\frac{X^{n-m-2}}{1.2.3\dots(n-m-2)}f^{(n-1)}a+\frac{X^{n-m-1}}{1.2.3\dots(n-m-2)(n-m-1)}f^{(n)}a+\dots$$

sera divergente, ce qui ne peut avoir lieu qu'en supposant

$$\lim.\left[\text{mod.}\frac{X^{n-m}}{1.2.3\dots(n-m-1)(n-m)}f^{(n)}a\right]^{\frac{1}{n}}_{n=\infty}<1;\ \lim.\left[\text{mod.}\frac{X^{n-m-1}}{1.2.3\dots(n-m-2)(n-m-1)}f^{(n)}a\right]^{\frac{1}{n}}_{n=\infty}<1.$$

Mais ces conditions peuvent être exprimées par

$$12.\quad\left\{\begin{array}{l}\lim.\left[\text{mod.}\frac{z^n}{1.2.3\dots(n-1)n}f^{(n)}a\right]^{\frac{1}{n}}_{n=\infty}<\lim.\left[\frac{(\text{mod.}\,z)^n}{(\text{mod.}\,X)^{n-m-1}}\cdot\frac{1}{(n-m+1)(n-m+2)\dots(n-1)n}\right]^{\frac{1}{n}}_{n=\infty}\\ \lim.\left[\text{mod.}\frac{z^n}{1.2.3\dots(n-1)n}f^{(n)}a\right]^{\frac{1}{n}}_{n=\infty}<\lim.\left[\frac{(\text{mod.}\,z)^n}{(\text{mod.}\,X)^{n-m-1}}\cdot\frac{1}{(n-m)(n-m+1)\dots(n-1)n}\right]^{\frac{1}{n}}_{n=\infty}.\end{array}\right.$$

Or

$$\lim.\left[\frac{(\text{mod.}\,z)^n}{(\text{mod.}\,X)^{n-m}}\cdot\frac{1}{(n-m+1)(n-m+2)\dots(n-1)n}\right]^{\frac{1}{n}}_{n=\infty}>\lim.\left[\left(\frac{\text{mod.}\,z}{\text{mod.}\,X}\right)^n\left(\frac{\text{mod.}\,X}{n}\right)^m\right]^{\frac{1}{n}}_{n=\infty};$$
$$\lim.\left[\frac{(\text{mod.}\,z)^n}{(\text{mod.}\,X)^{n-m}}\cdot\frac{1}{(n-m)(n-m+1)\dots(n-1)n}\right]^{\frac{1}{n}}_{n=\infty}>\lim.\left[\left(\frac{\text{mod.}\,z}{\text{mod.}\,X}\right)^n\left(\frac{\text{mod.}\,X}{n}\right)^{m+1}\right]^{\frac{1}{n}}_{n=\infty},$$

et

$$\lim.\left[\left(\frac{\text{mod.}\,z}{\text{mod.}\,X}\right)^n.\left(\frac{\text{mod.}\,X}{n}\right)^m\right]^{\frac{1}{n}}_{n=\infty}=\frac{\text{mod.}\,z}{\text{mod.}\,X}.\lim.\left[\frac{\text{mod.}\,X}{n}\right]^{\frac{m}{n}}_{n=\infty}=\frac{\text{mod.}\,z}{\text{mod.}\,X};$$
$$\lim.\left[\left(\frac{\text{mod.}\,z}{\text{mod.}\,X}\right)^n.\left(\frac{\text{mod.}\,X}{n}\right)^{m+1}\right]^{\frac{1}{n}}_{n=\infty}=\frac{\text{mod.}\,z}{\text{mod.}\,X}.\lim.\left[\frac{\text{mod.}\,X}{n}\right]^{\frac{m+1}{n}}_{n=\infty}=\frac{\text{mod.}\,z}{\text{mod.}\,X}:$$

donc les inégalités donneront

$$\lim.\left[\text{mod.}\frac{z^n}{1.2.3\dots(n-1)n}f^{(n)}a\right]^{\frac{1}{n}}_{n=\infty}>\frac{\text{mod.}\,z}{\text{mod.}\,X}.$$

En comparant cette inégalité avec la condition (2.) de la convergence de la série

$$fa+\frac{z}{1}f'a+\frac{z^2}{1.2}f''a+\frac{z^3}{1.2.3}f'''a+\dots+\frac{z^{n-1}}{1.2.3\dots(n-1)}f^{(n-1)}a$$
$$+\frac{z^n}{1.2.3\dots(n-1)n}f^{(n)}a+\dots$$

on voit que la série sera toujours divergente, si le module de x est plus grand que celui de la valeur de x qui rendrait infinie ou discontinue au moins une des fonctions

$$f(a+x),\quad f'(a+x),\quad f''(a+x),\ \ldots\ f^{(n-1)}(a+x),\quad f^{(n)}(a+x),\ \ldots$$

Nous voilà donc parvenus à ce théorème général:

„La série de ***Taylor:***

$$fa+\frac{z}{1}f'a+\frac{z^2}{1.2}f''a+\frac{z^3}{1.2.3}f'''a+\ldots+\frac{z^{n-1}}{1.2.3\ldots(n-1)}f^{(n-1)}a$$
$$+\frac{z^n}{1.2.3\ldots(n-1)n}f^{(n)}+\ldots$$

est divergente ou convergente suivant que le module de z est plus grand ou plus petit que celui de la valeur imaginaire x qui rendrait infinie ou discontinue au moins une des fonctions

$$f(a+x),\ f'(a+x),\ f''(a+x),\ \ldots\ f^{(n-1)}(a+x),\ f^{(n)}(a+x),\ \ldots\text{"}$$

C'est ainsi, par exemple, que la série

$$(1+z^2)^{\frac{3}{2}}=1+\tfrac{3}{2}z^2+\tfrac{3}{8}x^4-\tfrac{3}{8}(1-\tfrac{5}{6})z^6+\tfrac{3}{8}(1-\tfrac{5}{6})(1-\tfrac{5}{8})z^8-\tfrac{3}{8}(1-\tfrac{5}{6})(1-\tfrac{5}{8})(1-\tfrac{5}{10})z^{10}\ldots$$

est convergente ou divergente suivant que le module de la valeur de z est plus petit ou plus grand que l'unité qui est le module de la valeur $x=\sqrt{-1}$ pour laquelle la seconde dérivée et les suivantes de $(1+x^2)^{\frac{3}{2}}$ deviennent infinies.

Ce théorème n'est qu'une très simple conclusion des découvertes remarquables de Mr. *Cauchy;* mais il est en partie contraire à la règle de la convergence des séries donnée par cet illustre Géomètre, dont l'énoncé est le suivant:

„x designant une variable réelle ou imaginaire, une fonction réelle ou imaginaire de x sera développable en série convergente ordonnée suivant les puissances ascendantes de x, tant que le module de x conserve une valeur inférieure à la plus petite de celles pour lesquelles la fonction ou sa dérivée cesse d'être finie et continue." *)

L'insuffisance de cette règle provient, ce me sèmble, de ce que Mr. *Cauchy* suppose la valeur de l'intégrale définie être developpable en série convergente, lorsque la différentielle entre les limites de l'intégration peut être développée en série convergente; ce qui n'a lieu que dans des cas particuliers.

---

*) *Cauchy,* Exercices d'Analyse et de Physique Mathématique. Tome I. pag. 29.

23.

In determinationem coëfficientium $\overset{k}{C}_n$ in pag. 247 seqq. T. XXV. hujus Diarii relatarum.

(Auct. Dr. *E. G. Björling*, ad acad. Upsaliens. docens mathes.)

Celeb. *Grunert* in dissertatione quamvis excellenti „Über die Summirung „der Reihen von der Form etc." loco cit. pag. 250 — 255 tamen coëfficientes illas $\overset{k}{C}_n$ determinandi methodo usus est, ut facile patet, non omnino commodissima. Scilicet ut minime directa est minimoque particularis ista methodus, ita rem per se non parum simplicem facilique negotio perspicuum ultra modum extendit redditque diffusam, nec tamen legem quaesitam nisi *per inductionem* tandem sistit probatam. Ut nobis videtur, methodus, qua in sequentibus usi sumus, non modo caeteris promtior est magisque directa sed talis *quae unica,* dum fieri potest, in rebus *omnibus* praesenti similibus sit adhibenda.

Ex schemate in pag. 248 videtur esse (n et k denot. num. integros quascumque) absque exceptione

$$1.\quad \overset{k+1}{C}_n = n\overset{k}{C}_n + \overset{k}{C}_{n-1},$$

putatis nempe $=0$ iis C, quarum index inferior $=0$ nec non quarum index inferior superiori mojor sit; atque de caetero

$$2.\quad \overset{k}{C}_1 = 1 = \overset{k}{C}_k.$$

Quaeritur $\overset{k+1}{C}_n$ ***quaenam sit functio ipsorum*** k ***et*** n***, dum*** $n>1$ ***at*** $\gtreqless k$.

---

1) $\overset{k+1}{C}_2$. Ex (1.) concluditur ($k \gtreqless 2$)

$$\overset{k+1}{C}_2 = 2\overset{k}{C}_2 + 1,\quad \text{ideoque}\quad \Delta.\overset{k}{C}_2 = \overset{k}{C}_2 + 1;$$

de caetero $\overset{2}{C}_2 = 1$

Qua quidem aequatione differentiae integrati habetur

$$\overset{k}{C}_2 = 2^k.\Sigma(\tfrac{1}{2})^{k+1},$$
$$= 2^k(\text{const.} - (\tfrac{1}{2})^k);\quad \text{et, quoniam const.} = \tfrac{1}{2},$$
$$3.\quad = 2^{k-1} - 1;$$

ideoque

$$3'.\quad \overset{k+1}{C}_2 = 2^k - 1.$$

2) $\overset{k+1}{C}_3$. Ex (1.) et (3.) concluditur ($k \gtreqless 3$)

$$\overset{k+1}{C}_3 = 3\overset{k}{C}_3 + 2^{k-1} - 1, \quad \text{ideoque} \quad \Delta.\overset{k}{C}_3 = 2\overset{k}{C}_3 + 2^{k-1} - 1;$$

de caetero $\overset{3}{C}_3 = 1$.

Qua integrata habitur

$$\overset{k}{C}_3 = 3^k.\Sigma\frac{2^{k-1}-1}{3^{k+1}} = 3^{k-2}.\Sigma\{(\tfrac{2}{3})^{k-1} - (\tfrac{1}{3})^{k-1}\};$$

unde

$$4. \quad 2.\overset{k}{C}_3 = 3^{k-1} - 2.2^{k-1} + 1;$$

ideoque

$$4'. \quad 2.\overset{k+1}{C}_3 = 3^k - 2.2^k + 1.$$

3) $\overset{k+1}{C}_4$. Ex (1.) et (4.) concluditur ($k \gtreqless 4$)

$$\overset{k+1}{C}_4 = 4.\overset{k}{C}_4 + \frac{3^{k-1} - 2.2^{k-1} + 1}{2}, \quad \text{ideoque} \quad \Delta.\overset{k}{C}_4 = 3.\overset{k}{C}_4 + \frac{3^{k-1} - 2.2^{k-1} + 1}{2};$$

de caetero $\overset{4}{C}_4 = 1$.

Qua integrata habetur

$$2.\overset{k}{C}_4 = 4^k.\Sigma\frac{3^{k-1} - 2.2^{k-1} + 1}{4^{k+1}} = 4^{k-2}.\Sigma\{(\tfrac{3}{4})^{k-1} - 2(\tfrac{2}{4})^{k-1} + (\tfrac{1}{4})^{k-1}\};$$

unde

$$5. \quad 2.3.\overset{k}{C}_4 = 4^{k-1} - 3.3^{k-1} + 3.2^{k-1} - 1;$$

ideoque

$$5'. \quad 2.3.\overset{k+1}{C}_4 = 4^k - 3.3^k + 3.2^k - 1.$$

4) $\overset{k+1}{C}_5$. Ex (1.) et (5.) concluditur ($k \gtreqless 5$)

$$\overset{k+1}{C}_5 = 5.\overset{k}{C}_5 + \frac{4^{k-1} - 3.3^{k-1} + 3.2^{k-1} - 1}{2.3},$$

ideoque

$$\Delta.\overset{k}{C}_5 = 4.\overset{k}{C}_5 + \frac{4^{k-1} - 3.3^{k-1} + 3.2^{k-1} - 1}{2.3};$$

de caetero $\overset{5}{C}_5 = 1$.

Qua integrata habetur

$$2.3.\overset{k}{C}_5 = 5^k.\Sigma\frac{4^{k-1} - 3.3^{k-1} + 3.2^{k-1} - 1}{5^{k+1}} = 5^{k-3}.\Sigma\{(\tfrac{4}{5})^{k-1} - 3(\tfrac{3}{5})^{k-1} + 3(\tfrac{2}{5})^{k-1} - (\tfrac{1}{5})^{k-1}\};$$

unde

$$6. \quad 2.3.4.\overset{k}{C}_5 = 5^{k-1} - 4.4^{k-1} + 6.3^{k-1} - 4.2^{k-1} + 1;$$

ideoque

$$6'. \quad 2.3.4.\overset{k+1}{C}_5 = 5^k - 4.4^k + 6.3^k - 4.2^k + 1.$$

Jamque *per inductionem* licet concludi [$n>1, k \gtreqless n$]:

$$\Gamma(n).\overset{k+1}{C}_n = n^k - [n-1]_1{}^{*)}(n-1)^k + [n-1]_2(n-2)^k - \ldots + (-1)^{n-1}[n-1]_{n-1}.1^k,$$
$$= (-1)^{n-1}.\{1^k - [n-1]_1.2^k + [n-1]_2.3^k - \ldots + (-1)^{n-1}[n-1]_{n-1}.n^k\},$$
$$= (-1)^n.\{-1^k + [n-1]_1.2^k - [n-1]_2.3^k + \ldots + (-1)^n [n-1]_{n-1}.n^k\},$$
$$(7'.) \quad = (-1)^n.\overset{i=n}{\underset{i=1}{S}}(-1)^i[n-1]_{i-1}i^k,$$

nec non

$$(7.) \quad \Gamma(n).\overset{k}{C}_n = (-1)^n.\overset{i=n}{\underset{i=1}{S}}(-1)^i[n-1]_{i-1}i^{k-1}.$$

Eadem haec est ac aequatio penultima in pag. 255 loco cit. Sicuti haec, illa non nisi *per inductionem* est inventa at, ut plane apparet, via longe breviori atque naturae rei propria.

Veram hanc esse legem (7.) *seu* (7'.), *jam licet perfecte probari et quidem solito illo more* **). Scilicet antea probatum est, veram eam esse pro $\overset{k}{C}_2$, $\overset{k}{C}_3$, $\overset{k}{C}_4$, $\overset{k}{C}_5$ ($k \gtreqless$ indice inferiori).

---

*) Scilicet $[n-1]_i$ denotante, uti assolet, $\dfrac{(n-1)(n-2)\ldots(n-i)}{1.2.3\ldots i}$.

**) Veram eam esse pro aequalibus indicibus (inferiori et superiori), i. e. esse pro $k=n$ membrum posterius (7.) $=\Gamma(n)$, heic ante omnia liceat directe probari.

Est quidem

$$\text{membr. poster. (7.)} = (-1)^n \overset{i=n}{\underset{i=1}{S}} \frac{(-1)^i}{n}.\frac{n}{i}[n-1]_{i-1}i^k;$$

at

$$\frac{n}{i}[n-1]_{i-1} = \frac{n}{i}.\frac{(n-1)(n-2)\ldots(n-i+1)}{1\;.\;2\;\ldots\;(i-1)} = [n]_i,$$

ideoque

$$\text{membr. poster. (7.)} = \frac{(-1)^n}{n}\overset{i=n}{\underset{i=1}{S}}(-1)^i[n]_i i^k,$$

atque igitur, pro $k=n$,

$$= \frac{(-1)^n}{n}.\left\{-[n]_1.1^n + [n]_2.2^n - [n]_3.3^n + \ldots + (-1)^{n-1}[n]_{n-1}(n-1)^n + (-1)^n[n]_n n^n\right\},$$
$$= \frac{1}{n}.\left\{n^n - [n]_1(n-1)^n + [n]_2(n-2)^n - \ldots + (-1)^{n+1}[n]_1.1^n\right\},$$
$$= \frac{\Gamma(n+1)}{n} \text{ (vid. ex. gr. *Lacroix*, Calc. Diff. et Int. T. III. pag. 10)},$$
$$= \Gamma(n).$$

Posito jam, veram eam esse pro $\overset{k}{C}_2$, $\overset{k}{C}_3$, ... $\overset{k}{C}_p$ $(p<k)$, nos jam contendimus valere eandem pro $\overset{k}{C}_{p+1}$, i. e. esse

$$(A.)\qquad \overset{k}{C}_{p+1} = \frac{(-1)^{p+1}}{\Gamma(p+1)}\cdot\overset{i=p+1}{\underset{i=1}{S}}(-1)^i[p]_{i-1}\,i^{k-1}.$$

Ex (1.) concluditur $(k \overline{\gtrless} p+1)$

$$\overset{k+1}{C}_{p+1} = (p+1)\overset{k}{C}_{p+1}+\overset{k}{C}_p,$$

ideoque sec. (7.), quae quidem vera ad $\overset{k}{C}_p$ usque (inclusive) posita esset,

$$\overset{k+1}{C}_{p+1} = (p+1)\overset{k}{C}_{p+1}+\frac{(-1)^p}{\Gamma(p)}\cdot\overset{i=p}{\underset{i=1}{S}}(-1)^i[p-1]_{i-1}\,i^{k-1},$$

ideoque

$$\Delta.\overset{k}{C}_{p+1} = p\overset{k}{C}_{p+1}+\frac{(-1)^p}{\Gamma(p)}\cdot\overset{i=p}{\underset{i=1}{S}}(-1)^i[p-1]_{i-1}\,i^{k-1};$$

de caetero $\overset{p+1}{C}_{p+1}=1$.

Qua integrata habetur

$$\overset{k}{C}_{p+1} = (p+1)^k.\Sigma\frac{(-1)^p}{(p+1)^{k+1}.\Gamma(p)}\cdot\overset{i=p}{\underset{i=1}{S}}(-1)^i[p-1]_{i-1}\,i^{k-1},$$

seu

$$(B.)\qquad \Gamma(p).\overset{k}{C}_{p+1}$$
$$=(-1)^p(p+1)^{k-2}.\Sigma\overset{i=p}{\underset{i=1}{S}}(-1)^i[p-1]_{i-1}\left(\frac{i}{p+1}\right)^{k-1}$$
$$=(-1)^p(p+1)^{k-2}.\Sigma\Big\{-\left(\frac{1}{p+1}\right)^{k-1}+[p-1]_1\left(\frac{2}{p+1}\right)^{k-1}-[p-1]_2\left(\frac{3}{p+1}\right)^{k-1}+\dots\dots$$
$$\dots+(-1)^i[p-1]_{i-1}\left(\frac{i}{p+1}\right)^{k-1}+\dots+(-1)^p[p-1]_{p-1}\left(\frac{p}{p+1}\right)^{k-1}\Big\}.$$

Est autem

$$\Sigma(-1)^i[p-1]_{i-1}\left(\frac{i}{p+1}\right)^{k-1}$$

seu

$$(-1)^i[p-1]_{i-1}.\Sigma\left(\frac{i}{p+1}\right)^{k-1} = A-(-1)^i[p-1]_{i-1}.\frac{p+1}{p-i+1}\left(\frac{i}{p+1}\right)^{k-1},$$

(A denot. quant. ab k haud pendentem)

seu

$$= A+(-1)^{i+1}.\frac{(p-1)(p-2)\dots(p-i+1)}{1\;.\;2\;\dots\;(i-1)}\cdot\frac{p+1}{p-i+1}\cdot\left(\frac{i}{p+1}\right)^{k-1},$$
$$= A+(-1)^{i+1}.\frac{p+1}{p}.[p]_{i-1}\left(\frac{i}{p+1}\right)^{k-1} = A+\frac{(-1)^{i+1}}{p(p+1)^{k-2}}[p]_{i-1}\,i^{k-1}.$$

Itaque secundum (B.), quoniam $p\Gamma(p)=\Gamma(p+1)$, habetur

$$\Gamma(p+1).\overset{k}{C}_{p+1} = (p+1)^{k-2}.A'+(-1)^{p+1}.\overset{i=p}{\underset{i=1}{S}}(-1)^i[p]_{i-1}\,i^{k-1},$$

A' denot. quant. ab k haud pendentem, quam facillimo jam licet negotio inveniri. Scil. quoniam $\overset{p+1}{C}_{p+1} = 1$, habetur ex aequat. novissima haecce relatio:

$$(p+1)^{p-1}.A' = \Gamma(p+1)+(-1)^p \overset{i=p}{\underset{i=1}{S}}(-1)^i [p]_{i-1}\, i^p,$$

seu, quoniam $(p+1)\,\Gamma(p+1) = \Gamma(p+2)$ et $(p+1)\,[p]_{i-1}\, i^p = [p+1]_i . i^{p+1}$, haecce:

$$(p+1)^p.A' = \Gamma(p+2)+(-1)^p.\overset{i=p}{\underset{i=1}{S}}(-1)^i [p+1]_i . i^{p+1},$$

vel etiam, quoniam valor termini novissimi pro $i = p+1$ est $= -(p+1)^{p+1}$,

$$(p+1)^p.A' = (p+1)^{p+1}+\Gamma(p+2)+(-1)^p.\overset{i=p+1}{\underset{i=1}{S}}(-1)^i [p+1]_i . i^{p+1};$$

qui autem terminus novissimus, ut in notula praecedente monuimus, est $= -\Gamma(p+2)$. Itaque

$$A' = p+1,$$

tandemque

$$\Gamma(p+1).\overset{k}{C}_{p+1} = (p+1)^{k-1}+(-1)^{p+1}.\overset{i=p}{\underset{i=1}{S}}(-1)^i [p]_{i-1}\, i^{k-1},$$
$$= (-1)^{p+1}.\overset{i=p+1}{\underset{i=1}{S}}(-1)^i [p]_{i-1}\, i^{k-1}.$$

Q. E. D.

Upsaliae d. XX Sept. 1843.

Facsimile einer Handschrift von Roberval.

J'ay quatre choses a repliquer à Monsieur des Cartes.
1° J'advoue que je me suis trompé dans
l'escrit que j'ay faict [illegible]
mais scavez vous en quoy? c'est que je croyois
qu'il fust amateur de la verité: et au contraire
je recognois maintenant qu'aussi tost qu'elle ne
s'accorde pas à ses pensees, et la combat, il declare son
adversaire [illegible]

Mais je differe à la [illegible] tendant pas se dedire; une mauvaise cause;

24.

Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Enstehung verdanken.

(Von Herrn Stud. *Gotth. Eisenstein* zu Berlin.)

Darstellung des Ausdrucks $27.\frac{x^p-1}{x-1}$ durch eine cubische Form mit drei Variabeln.

§. 1.

Es ist bekannt, dafs für jede Primzahl p der Ausdruck

$$(1.)\qquad X = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+x+1$$

auf die Form

$$(2.)\qquad \tfrac{1}{4}[Y^2-(-1)^{\frac{1}{2}(p-1)}pZ^2],$$

gebracht werden kann, wo Y und Z ganze Functionen von x mit ganzen Coëfficienten sind; und man weifs, dafs diese Zerfällung von der Zerlegung der Gesammtheit Ω der Wurzeln der Gleichung

$$(3.)\qquad \frac{x^p-1}{x-1} = 0$$

in zwei Perioden abhängt. — Wir wollen uns in dieser Abhandlung zuerst mit einer neuen Zerfällung desselben Ausdrucks X beschäftigen, welche der Zerlegung von Ω in *drei* Perioden für eine Primzahl p von der Form $3m+1$ ihre Entstehung verdankt. Die Form dieser neuen Zerfällung, unabhängig von der Art ihrer Entstehung aufgefafst, wird später auf eine ganze Reihe von neuen und umfassenden Resultaten führen.

Wenn p eine Primzahl von der Form $3m+1$ ist, so sind bekanntlich diese drei Perioden die Wurzeln der cubischen Gleichung

$$y^3+y^2-\tfrac{1}{3}(p-1)y-C = 0,$$

wo

$$4p = M^2+3N^2,\quad N\equiv 0 \pmod 3 \text{ und}$$
$$C = \tfrac{1}{27}\left(3p-1+\left(\tfrac{M}{3}\right)Mp\right)$$

gesetzt ist. Diese Gleichung vereinfacht sich, wenn man

$$z = 3y+1$$

setzt, und man erhält die folgende Gleichung in z:

$$z^3 = 3pz + \left(\frac{M}{3}\right)Mp.$$

Diese reducirte cubische Gleichung, auf die gewöhnliche Weise aufgelöset, würde die Werthe der drei Perioden liefern. Indessen bedürfen wir gar nicht der Kenntnifs der cubischen Gleichung, zu welcher man nur auf einem ziemlich complicirten Wege gelangt, sondern man kann durch höchst einfache Betrachtungen, wie wir sie schon in den „Beiträgen zur Kreistheilung" und in dem „Beweise des cubischen Reciprocitätsgesetzes" angestellt haben, die Werthe der drei Perioden *a priori* bestimmen.

In der That: es sei r eine Wurzel der Gleichung (3.), ϱ eine imaginäre Cubikwurzel der Einheit und man setze

$$\sum_{k=1}^{k=p-1} \varrho^{\text{Ind.}k}\, r^{ak} = \varphi(a),$$

$$\sum_{k=1}^{k=p-1} \varrho^{2\,\text{Ind.}k}\, r^{ak} = \psi(a),$$

wo Ind. k sich auf die Primzahl p und auf eine nach Belieben angenommene primitive Congruenzwurzel g bezieht, und wo a irgend eine nicht durch p theilbare ganze Zahl vorstellt. Setzt man

$$ak \equiv t \pmod{p}, \quad t < p, \quad \text{woraus}$$

$$\text{Ind.}a + \text{Ind.}k \equiv \text{Ind.}t \pmod{p-1} \text{ folgt, so wird}$$

$$r^{ak} = r^t, \quad \varrho^{\text{Ind.}k} = \varrho^{-\text{Ind.}a}\varrho^{\text{Ind.}t}, \quad \varrho^{2\,\text{Ind.}k} = \varrho^{-2\,\text{Ind.}a}\varrho^{2\,\text{Ind.}t},$$

während t wiederum die Werthe

$$1,\ 2,\ 3\ \ldots\ldots\ p-1\ (\mu)$$

durchläuft: also erhält man

$$(4.)\qquad \varphi(a) = \varrho^{-\text{Ind.}a}\sum_{t=1}^{t=p-1}\varrho^{\text{Ind.}t}\, r^t = \varrho^{2\,\text{Ind.}a}\varphi(1),$$

$$\psi(a) = \varrho^{-2\,\text{Ind.}a}\sum_{t=1}^{t=p-1}\varrho^{2\,\text{Ind.}t}\, r^t = \varrho^{\text{Ind.}a}\psi(1).$$

Das Product der beiden Reihen $\varphi(1)$ und $\psi(1)$ ist

$$\varphi(1)\psi(1) = \sum_{s=1}^{s=p-1}\sum_{t=1}^{t=p-1}\varrho^{\text{Ind.}s-\text{Ind.}t}\, r^{s+t}.$$

Stellt man sich in dieser Doppelsumme unter s auf einen Augenblick einen stehenden Werth vor und setzt $t \equiv sk \pmod{p}$, $k < p$, woraus Ind. s — Ind. t $\equiv$ — Ind. $k \pmod{p-1}$ folgt, so erhält man, weil nun k selbst wieder für jeden Werth von s die Werthe (μ) durchläuft,

$$\varphi(1)\psi(1) = \sum_{s=1}^{s=p-1}\sum_{k=1}^{k=p-1}\varrho^{-\text{Ind.}k}\, r^{s(1+k)}$$

Die Summation nach s läfst sich jetzt ausführen, und man erhält für jeden Werth von k, mit Ausnahme des einzigen $k=p-1$:

$$\sum_{s=1}^{s=p-1} r^{s(1+k)} = r+r^2+\ldots+r^{p-1} = -1;$$

dagegen für $k=p-1$, weil in diesem speciellen Falle $1+k=p$, also $r^{1+k}=1$ ist,

$$\text{dieselbe Summe} = 1+1+\ldots+1 = p-1.$$

Im Ganzen erhält man also

$$\varphi(1)\psi(1) = -\sum_{k=1}^{k=p-1} \varrho^{-\text{Ind.}k} + p.\varrho^{-\text{Ind.}(p-1)}.$$

Die Summe nach k verschwindet, weil Ind. k die Werthe 0, 1, 2, ... $p-4$, $p-3$, $p-2$ durchläuft; aufserdem ist $\text{Ind.}(p-1)=\frac{1}{2}(p-1)$ durch 3 theilbar, also $\varrho^{-\text{Ind.}(p-1)}=1$, folglich giebt die eben erhaltene Gleichung

$$(5.)\quad \varphi(1)\psi(1) = p.$$

Man bilde ferner das Quadrat der Reihe $\varphi(1)$, nämlich:

$$\varphi(1)^2 = \sum_{s=1}^{s=p-1}\sum_{t=1}^{t=p-1} \varrho^{\text{Ind.}s+\text{Ind.}t} r^{s+t}.$$

Stellt man sich unter s einen stehenden Werth vor, setzt $t\equiv sk$ (mod. p), $k<p$, woraus $\text{Ind.}t\equiv\text{Ind.}s+\text{Ind.}k$ (mod. $p-1$) folgt, und bedenkt, dafs nun k für jeden Werth von s die Werthe (μ) durchläuft, so geht die Gleichung in

$$\varphi(1)^2 = \sum_{s=1}^{s=p-1}\sum_{k=1}^{k=p-1} \varrho^{2\,\text{Ind.}s+\text{Ind.}k} r^{s(1+k)}$$

über. Aber nach (4.) ist $\sum_{s=1}^{s=p-1} \varrho^{2\,\text{Ind.}s} r^{(k+1)s} = \varrho^{\text{Ind.}(k+1)}\psi(1)$, für alle Werthe von k; nur nicht für $k=p-1$; in welchem Falle dieselbe Summe offenbar verschwindet. Es tritt daher $\psi(1)$ als gemeinschaftlicher Factor aller Glieder heraus und man erhält

$$\varphi(1)^2 = \psi(1)\sum_{k=1}^{k=p-2} \varrho^{\text{Ind.}k+\text{Ind.}(k+1)}.$$

Die Reihe $\sum_{k=1}^{k=p-2} \varrho^{\text{Ind.}k+\text{Ind}(k+1)}$ läfst sich offenbar auf die Form $a+b\varrho$ bringen, wo a und b reelle ganze Zahlen sind; sie ist also einer ganzen complexen Zahl gleich, welche aus dritten Wurzeln der Einheit zusammengesetzt ist, und man erhält

$$(6.)\quad \frac{\varphi(1)^2}{\psi(1)} = \sum_{k=1}^{k=p-2} \varrho^{\text{Ind.}k+\text{Ind.}(k+1)} = a+b\varrho.$$

Auf dieselbe Weise kommt

$$(7.)\quad \frac{\psi(1)^2}{\varphi(1)} = \sum_{k=1}^{k=p-2} \varrho^{2\,\text{Ind.}k+2\,\text{Ind.}(k+1)} = a+b\varrho^2.$$

Multiplicirt man diese beiden Resultate (6.) und (7.) mit einander und bemerkt, dafs nach (5.) $\varphi(1)\psi(1) = p$ ist, so erhält man

$$(8.)\qquad (a+b\varrho)(a+b\varrho^2) = p,$$

woraus zu ersehen, dafs die reelle Primzahl p von der Form $3m+1$ sich in das Product zweier ganzen complexen Zahlen aus dritten Wurzeln der Einheit zerlegen läfst. Die beiden ganzen complexen Zahlen $a+b\varrho$ und $a+b\varrho^2$ sind durch die Bedingung, dafs ihre gemeinschaftliche Norm $=p$ ist, noch nicht vollständig bestimmt. Um sie vollständig zu bestimmen, bemerke man, dafs nach (6.) $\varphi(1)^3 = \varphi(1)\psi(1)(a+b\varrho) = p(a+b\varrho)$ ist. Entwickelt man den Cubus der Reihe $\varphi(1)$ nach dem polynomischen Satze, so giebt diese Entwicklung erstlich die Cuben aller einzelnen Glieder der Reihe, und dann noch Glieder, deren Coëfficienten sämmtlich durch 3 theilbar sind. Die Summe der Cuben der einzelnen Glieder ist, wegen $\varrho^3 = 1$, $= \sum\limits_{k=1}^{k=p-1} r^{3k} = -1$, und man erhält eine Gleichung von der Form

$$-1+3L = p(a+b\varrho), \quad \text{wo} \quad L = A+Br+Cr^2 \ldots. \text{ ist}$$

und A, B, C, ... ganze complexe Zahlen sind. Es folgt hieraus die Congruenz

$$p(a+b\varrho) \equiv -1 \pmod{3}, \quad \text{aber} \quad p \equiv 1 \pmod{3}, \quad \text{folglich}$$

$$(9.)\qquad a+b\varrho \equiv -1 \pmod{3}, \quad \text{ebenso} \quad a+b\varrho^2 \equiv -1 \pmod{3}\ ^{*}).$$

Jede ganze complexe Zahl von der Form $A+B\varrho$ (A und B reell und ganz), welche $\equiv -1$ (mod. 3) ist, heifse eine *primäre* complexe Zahl. Da jede ganze complexe Zahl l, welche nicht durch 3 und auch nicht durch $1-\varrho$ theilbar ist, nur einer der sechs Einheiten

$$1, \quad \varrho, \quad \varrho^2, \quad -1, \quad -\varrho, \quad -\varrho^2$$

nach dem mod. 3 congruent sein kann, so sieht man, dafs sich unter sechs associirten complexen Zahlen, wie

$$l, \quad \varrho l, \quad \varrho^2 l, \quad -l, \quad -\varrho l, \quad -\varrho^2 l,$$

immer eine und nur eine *primäre* befinden wird. Zerlegt man also die Primzahl p in das Product $p_1 p_2$ ihrer beiden primären complexen Primfactoren p_1 und p_2, so geben diese letzteren die Werthe von $a+b\varrho$ und $a+b\varrho^2$. Es bleibt nur noch zu entscheiden, welche von den beiden complexen Zahlen $a+b\varrho$

*) Da L eine ganze Function der Wurzeln der Gleichung (3.) mit ganzen complexen Coëfficienten ist, und da zugleich L einer rationalen complexen Zahl gleich wird, so mufs L nothwendig einer ganzen complexen Zahl gleich sein. Man sehe deshalb die Hülfssätze zu dem „Beweise des cub. Reciprocitätsgesetzes."

und $a+b\varrho^2$ gleich p_1, und welche gleich p_2 zu setzen sei. Zu dem Ende bezeichne man durch p_1 denjenigen der beiden primären Primfactoren, in welche man p *a priori* zerlegt hat und für welchen die Congruenz $k^{\frac{1}{3}(p-1)} \equiv \varrho^{\text{Ind.}\,k} (\text{mod.}\, p_1)$ erfüllt wird, während dann für den andern $k^{\frac{1}{3}(p-1)} \equiv \varrho^{2\,\text{Ind.}\,k} (\text{mod.}\, p_2)$ sein wird.

Unter dieser Voraussetzung erhält man

$$a+b\varrho = \sum_{k=1}^{k=p-2} \varrho^{\text{Ind.}\,k} \varrho^{\text{Ind.}(k+1)} \equiv \sum_{k=1}^{k=p-2} k^{\frac{1}{3}(p-1)}(k+1)^{\frac{1}{3}(p-1)} \ (\text{mod.}\, p_1).$$

Aber der Werth der zweiten Summe ist eine reelle ganze Zahl und durch p theilbar, wovon man sich leicht überzeugt, wenn man in der Summe

$$\sum_{k=1}^{k=p-1} k^{\frac{1}{3}(p-1)}(k+1)^{\frac{1}{3}(p-1)},$$

welche sich von der obigen nur durch Vielfache von p unterscheidet, $(k+1)^{\frac{1}{3}(p-1)}$ nach dem binomischen Satze entwickelt; worauf jede der einzelnen Partialsummen, in die hierdurch die Summe zerfällt, durch p theilbar ist. Die obige Summe ist also um so mehr noch durch p_1 theilbar; folglich ist auch $a+b\varrho$ durch p_1 theilbar. Wäre nun $a+b\varrho = p_2$, so müfste p_2 durch p_1 theilbar sein; was unmöglich ist, da p_1 und p_2 conjugirte complexe Primzahlen sind *); also ist nothwendig $a+b\varrho = p_1$.

Man erhält daher

$$\varphi(1)^3 = pp_1, \quad \psi(1)^3 = pp_2, \quad \text{folglich}$$

$$(10.) \quad \sum_{k=1}^{k=p-1} \varrho^{\text{Ind.}\,k} r^k = \sqrt[3]{(pp_1)},$$

$$(11.) \quad \sum_{k=1}^{k=p-1} \varrho^{2\,\text{Ind.}\,k} r^k = \sqrt[3]{(pp_2)};$$

wo die beiden Cubikwurzeln so zu wählen sind, dafs ihr Product

$$\sqrt[3]{(pp_1)}\sqrt[3]{(pp_2)} = \varphi(1)\psi(1) = p \ \text{ wird.}$$

Diese beiden Gleichungen werden nun sogleich die Werthe der drei Perioden liefern.

Man bezeichne durch P die Summe aller Wurzeln $e^{\frac{2k\pi}{p}i}$ der Gleichung (3.), für welche Ind. k durch 3 theilbar ist; durch P' die Summe derjenigen Wurzeln derselben Gleichung, für welche Ind. $k \equiv -1$ (mod. 3) ist; endlich durch P'' die Summe aller der Wurzeln $e^{\frac{2k\pi}{p}i}$, für welche Ind. $k \equiv 1$ (mod. 3.) ist.

---

*) Nur die beiden conjugirten complexen Primzahlen $1-\varrho$ und $1-\varrho^2$, deren gemeinschaftliche Norm die Zahl 3 ist, theilen sich gegenseitig.

Setzt man $r = e^{\frac{2\pi}{p}i}$, so lassen sich die Gleichungen (10.) und (11.) folgendermafsen schreiben:

$$P + \varrho^2 P' + \varrho P'' = \sqrt[3]{(pp_1)},$$
$$P + \varrho P' + \varrho^2 P'' = \sqrt[3]{(pp_2)}.$$

Da sich zu diesen beiden Gleichungen noch die folgende gesellt:

$$P + P' + P'' = -1,$$

so haben wir jetzt ein System von linearen Gleichungen, welches sich nach P, P', P'' als Unbekannten auflösen läfst. Die Auflösung dieser Gleichungen liefert folgendes Resultat:

Lehrsatz 1.

„*Wenn man die reelle Primzahl p von der Form* $3m+1$ *in* „*das Product ihrer beiden primären, aus dritten Wurzeln der Ein-* „*heit zusammengesetzten complexen Primfactoren zerlegt und den-* „*jenigen von beiden, welcher für eine vorher nach Belieben ange-* „*nommene primitive Congruenzwurzel g die Congruenz* $g^{\frac{1}{3}(p-1)} \equiv \varrho$ „*(mod.* p_1*) erfüllt, durch* p_1, *den andern durch* p_2 *bezeichnet, so sind* „*die drei Perioden P, P', P'' durch die folgenden Gleichungen ge-* „*geben:*

$$3P = -1 + \sqrt[3]{(pp_1)} + \sqrt[3]{(pp_2)},$$
$$3P' = -1 + \varrho\sqrt[3]{(pp_1)} + \varrho^2\sqrt[3]{(pp_2)},$$
$$3P'' = -1 + \varrho^2\sqrt[3]{(pp_1)} + \varrho\sqrt[3]{(pp_2)};$$

„*wo die beiden Cubikwurzeln so zu wählen sind, dafs ihr Product* „*reell und der Primzal p gleich wird.*"

Bezeichnet man durch das Symbol $\left[\frac{k}{p_1}\right]$ diejenige Potenz von ϱ, welche $\equiv k^{\frac{1}{3}(p-1)}$ (mod. p_1) ist, so hat man $\varrho^{\text{Ind.}k} = \left[\frac{k}{p_1}\right]$, und man kann jetzt aus dem Resultate die primitive Congruenzwurzel und die Indices vollständig eliminiren und demselben folgende unabhängige Form geben.

„Die reelle Primzahl $p \equiv 1$ (mod. 3) sei in das Product ihrer beiden primären complexen Primfactoren p_1 und p_2 zerlegt; man bezeichne durch

$$P,\ P',\ P''$$

die Summe aller derjenigen Wurzeln $e^{\frac{2k\pi i}{p}}$ der Gleichung (3.), für welche respective

$$\left[\frac{k}{p_1}\right]=1,\quad \left[\frac{k}{p_1}\right]=\varrho^2,\quad \left[\frac{k}{p_1}\right]=\varrho$$

ist: so hat man

$$3P = -1+ \sqrt[3]{(pp_1)}+ \sqrt[3]{(pp_2)},$$
$$3P' = -1+ \varrho\sqrt[3]{(pp_1)}+\varrho^2\sqrt[3]{(pp_2)},$$
$$3P''= -1+\varrho^2\sqrt[3]{(pp_1)}+ \varrho\sqrt[3]{(pp_2)};$$

wo die beiden Cubikwurzeln $\sqrt[3]{(pp_1)}$ und $\sqrt[3]{(pp_2)}$ so zu wählen sind, dafs ihr Product $=p$ wird."

Wir denken uns p_1 immer so bestimmt, dafs der Coëfficient von ϱ *positiv*, also der Coëfficient von ϱ^2 in p_2 ebenfalls *positiv* ist. (Vergl. die Tabelle §. 3.)

§. 2.

Nachdem die Werthe der drei Perioden P, P', P'' gefunden sind, können wir die Function $X=\frac{x^p-1}{x-1}$ in das Product dreier ganzen Functionen ξ, η, ζ von x zerfällen, deren Coëfficienten aus P, P', P'' *linear* zusammengesetzt sind. Ordnet man diese drei Factoren, statt nach den Potenzen von x, vielmehr auf die Weise, dafs man alle Glieder zusammenfafst, welche respective mit P, P', P'' multiplicirt sind, so nehmen sie die Form

$$\xi = A+BP+CP'+DP''$$

an, wo A, B, C, D ganze Functionen von x mit ganzen reellen Coëfficienten sind, und es folgt aus der von *Gaufs* gegebenen Theorie, dafs, wenn ξ diesen Werth hat, die Werthe von η, ζ sogleich hieraus durch cyclische Permutation von P, P', P'' gefunden werden, nämlich:

$$\eta = A+BP'+CP''+DP,$$
$$\zeta = A+BP''+CP+DP'.$$

Man kann mit Hülfe der identischen Gleichung

$$1+P+P'+P'' = 0$$

einen beliebigen der vier Coëfficienten herausschaffen. Will man z. B. D eliminiren, so subtrahire man von den obigen Ausdrücken für ξ, η, ζ den folgenden:

$$0 = D+DP+DP'+DP'',$$

und man erhält

$$\xi = A-D+(B-D)P+(C-D)P',$$
$$\eta = A-D+(B-D)P'+(C-D)P'',$$
$$\zeta = A-D+(B-D)P''+(C-D)P;$$

so dafs also ξ, η, ζ immer auf die Form

$$(1.)\quad \xi = A + BP + CP', \quad \eta = A + BP' + CP'', \quad \zeta = A + BP'' + CP$$

gebracht werden können, wo A, B, C ganze Functionen von x mit ganzen reellen Coëfficienten sind.

Setzt man nun in diese Ausdrücke die Werthe der drei Perioden, wie sie sich oben ergeben haben, nämlich:

$$P = \tfrac{1}{3}(-1 + \sqrt[3]{(pp_1)} + \sqrt[3]{(pp_2)}),$$
$$P' = \tfrac{1}{3}(-1 + \varrho\sqrt[3]{(pp_1)} + \varrho^2\sqrt[3]{(pp_2)}),$$
$$P'' = \tfrac{1}{3}(-1 + \varrho^2\sqrt[3]{(pp_1)} + \varrho\sqrt[3]{(pp_2)}),$$

so erhält man

$$3\xi = 3A - B - C + B(\sqrt[3]{(pp_1)} + \sqrt[3]{(pp_2)}) + C(\varrho\sqrt[3]{(pp_1)} + \varrho^2\sqrt[3]{(pp_2)}),$$
$$3\eta = 3A - B - C + B(\varrho\sqrt[3]{(pp_1)} + \varrho^2\sqrt[3]{(pp_2)}) + C(\varrho^2\sqrt[3]{(pp_1)} + \varrho\sqrt[3]{(pp_2)}),$$
$$3\zeta = 3A - B - C + B(\varrho^2\sqrt[3]{(pp_1)} + \varrho\sqrt[3]{(pp_2)}) + C(\sqrt[3]{(pp_1)} + \sqrt[3]{(pp_2)});$$

welches sich auch folgendermafsen schreiben läfst:

$$(2.)\quad \begin{cases} 3\xi = U + Y\sqrt[3]{(pp_1)} + Z\sqrt[3]{(pp_2)}, \\ 3\eta = U + Y\varrho\sqrt[3]{(pp_1)} + Z\varrho^2\sqrt[3]{(pp_2)}, \\ 3\zeta = U + Y\varrho^2\sqrt[3]{(pp_1)} + Z\varrho\sqrt[3]{(pp_2)}, \\ Y = V + W\varrho, \quad Z = V + W\varrho^2; \end{cases}$$

wo U, V, W drei ganze Functionen von x mit ganzen reellen Coëfficienten sind. Multiplicirt man die drei Ausdrücke 3ξ, 3η, 3ζ wirklich ineinander, mit Hülfe der Formel

$$(\lambda + \mu + \nu)(\lambda + \varrho\mu + \varrho^2\nu)(\lambda + \varrho^2\mu + \varrho\nu) = \lambda^3 + \mu^3 + \nu^3 - 3\lambda\mu\nu,$$

und bemerkt, dafs $\sqrt[3]{(pp_1)} \cdot \sqrt[3]{(pp_2)} = p$ ist, so kommt

$$(3.)\quad 27\xi\eta\zeta = U^3 + pp_1 Y^3 + pp_2 Z^3 - 3p\,UYZ.$$

Lehrsatz 2.

„*Für jede Primzahl p von der Form $3m+1$ läfst sich also der*
„*Ausdruck*

$$„27(x^{p-1} + x^{p-2} + \ldots + x + 1)$$

„*auf die Form*

$$„U^3 + pp_1 Y^3 + pp_2 Z^3 - 3p\,UYZ,$$

„*bringen, wo $Y = V + W\varrho$, $Z = V + W\varrho^2$ ist und U, V, W ganze*
„*Functionen von x mit ganzen reellen Coëfficienten sind.*"

Ich bemerke noch, dafs man immer

$$U + V + W \equiv 0 \pmod{3}$$

hat; denn es ist $U + V + W = 3A$.

Beispiele. Für $p=7$ ist $p_1=2+3\varrho$, $p_2=2+3\varrho^2$, $U=3x^2+x+3$, $V=-x$, $W=0$.

Für $p=13$ ist $p_1=-1+3\varrho$, $p_2=-1+3\varrho^2$, $U=3x^4+x^3+5x^2+x+3$, $V=-x^3-x^2-x$, $W=-x^2$.

Mit Hülfe des Newtonschen Satzes über die Potenzsummen der Wurzeln einer Gleichung kann man durch Anwendung des symbolischen Zeichens $\left[\frac{k}{p_1}\right]$ allgemein die Coëfficienten der drei Polynome U, V, W durch analytische Formeln ausdrücken. Ein Umstand, auf den ich bei dieser Entwicklung im Vorbeigehn aufmerksam mache, besteht darin, dafs die Coëfficienten, wie sie die Formeln liefern, als Brüche erscheinen, ohne dafs man sieht, wie die Nenner durch die Zähler aufgehoben werden. Da man aber *a priori* weifs, dafs diese Coëfficienten ganze Zahlen sein müssen, so erhält man hieraus eine Reihe merkwürdiger Sätze über die Symbole von der Form $\left[\frac{k}{p_1}\right]$, welche in ihrer Verbindung zu dem cubischen Reciprocitätsgesetze und den Criterien des cubischen Characters der Zahl 3 führen, also die ganze Theorie der cubischen Reste implicite enthalten.

Eigenschaften der Ausdrücke von der Form Φ.

§. 3.

Die Ausdrücke von der Form

$$(1.)\quad u^3+pp_1y^3+pp_2z^3-3puyz = \Phi,$$

in welchen wir $y=v+w\varrho$, $z=v+w\varrho^2$ und u, v, w als reelle ganze Zahlen voraussetzen, und welche unter dieser Annahme nur reelle ganze Zahlen darstellen können, besitzen merkwürdige Eigenschaften. Die Fundamental-Eigenschaft derselben besteht darin, dafs je zwei Ausdrücke von dieser Form, mit einander multiplicirt, wieder einen Ausdruck von der nämlichen Form reproduciren. Es seien

$$\Phi = u^3+pp_1y^3+pp_2z^3-3puyz,$$
$$\Phi' = u'^3+pp_1y'^3+pp_2z'^3-3pu'y'z'$$

zwei Ausdrücke von dieser Form. Um nun das Product $\Phi\Phi'=\Phi''$ zu bilden, schreibe man Φ und Φ' wie folgt:

$$\Phi = (u+y\sqrt[3]{(pp_1)}+z\sqrt[3]{(pp_2)})(u+y\varrho\sqrt[3]{(pp_1)}+z\varrho^2\sqrt[3]{(pp_2)})$$
$$\times(u+y\varrho^2\sqrt[3]{(pp_1)}+z\varrho\sqrt[3]{(pp_2)}),$$

$$\Phi' = (u'+y'\sqrt[3]{(pp_1)}+z'\sqrt[3]{(pp_2)})(\text{etc.})(\text{etc.}),$$

und multiplicire je zwei übereinander stehende Factoren wirklich mit einander. Auf diese Weise erhält man offenbar einen Ausdruck, der genau dieselbe Gestalt hat, wie Φ und Φ', aber mit neuen Variabeln u'', y'', z'', nämlich:

$$(2.)\quad \begin{cases} u'' = uu'+pyz'+pzy', \\ y'' = uy'+yu'+p_2zz', \\ z'' = uz'+zu'+p_1yy', \end{cases}$$

und man sieht, dafs man, wenn $y=v+w\varrho$, $z=v+w\varrho^2$, $y'=v'+w'\varrho$, $z'=v'+w'\varrho^2$ gesetzt wird, $y''=v''+w''\varrho$, $z''=v''+w''\varrho^2$ erhält, und dafs u'', v'', w'' ebenfalls ganze Zahlen sein werden.

Man kann hieraus sogleich einige interessante Folgerungen ziehen. Wenn die unbestimmte Gleichung

$$(3.)\quad u^3+pp_1y^3+pp_2z^3-3puyz = 1,$$

für $y=v+w\varrho$, $z=v+w\varrho^2$, in reellen ganzen Zahlen u, v, w lösbar ist (mit Ausnahme der evidenten Lösung $u=1$, $y=z=0$), so lassen sich, wie bei der bekannten *Pell*schen Gleichung, *aus einer Lösung unendlich viele*, und hier sogar *doppelt* unendlich viele, ableiten. In der That: wenn u, y, z irgend ein System ist, welches der Gleichung (3.) genügt, so darf man nur

$$(4.)\quad (u+y\sqrt[3]{(pp_1)}+z\sqrt[3]{(pp_2)})^m(u+y\varrho\sqrt[3]{(pp_1)}+z\varrho^2\sqrt[3]{(pp_2)})^n \\ = U+Y\sqrt[3]{(pp_1)}+Z\sqrt[3]{(pp_2)}$$

setzen, wo m und n irgend welche positive oder negative ganze Zahlen vorstellen, und alle diese Systeme

$$U,\quad Y,\quad Z,$$

welche den verschiedenen Werthen von m und n entsprechen, werden ebenfalls der Gleichung (3.) Genüge thun.

Wenn M eine ganze Zahl vorstellt, welche durch die Form Φ repräsentirt werden kann, und man kennt alle Auflösungen der Gleichung (3.), so lassen sich aus einer Darstellung unendlich viele ableiten. Hat man z. B.

$$M = \alpha^3+pp_1\beta^3+pp_2\gamma^3-3p\alpha\beta\gamma,$$

und stellen

$$U,\quad Y,\quad Z$$

alle Systeme vor, welche der Gleichung (3.) genügen, so setze man

$$(5.)\quad (\alpha+\beta\sqrt[3]{(pp_1)}+\gamma\sqrt[3]{(pp_2)})(U+Y\sqrt[3]{(pp_1)}+Z\sqrt[3]{(pp_2)}) \\ = A+B\sqrt[3]{(pp_1)}+\Gamma\sqrt[3]{(pp_2)},$$

und es ist dann ebenfalls

$$M = A^3+pp_1B^3+pp_2\Gamma^3-3pAB\Gamma.$$

Zugleich sieht man, dafs sich alle Darstellungen, die man auf diese Weise erhält und die wir als eine *Gruppe* von Darstellungen bezeichnen, A, B, Γ in eine derselben α, β, γ lineär ausdrücken lassen; man darf zu dem Ende nur die linke Seite der Formel (5.) entwickeln, den reellen Theil dem reellen Theile und die Coëfficienten von resp. $\sqrt[3]{(pp_1)}$, $\sqrt[3]{(pp_2)}$ einander gleich setzen. Bei diesen Rechnungen hat man immer die einfachen Gleichungen

$$\eta\vartheta = p,\quad \eta^2 = p_1\vartheta,\quad \vartheta^2 = p_2\eta,\quad \eta^3 = pp_1,\quad \vartheta^3 = pp_2,\quad p_1p_2 = p$$

im Auge zu behalten, wo hier, wie im Folgenden, der Kürze halber die häufig vorkommenden Cubikwurzeln $\sqrt[3]{(pp_1)}$, $\sqrt[3]{(pp_2)}$ resp. durch η, ϑ bezeichnet werden.

Wenn die beiden ganzen Zahlen M und M' durch die Form Φ darstellbar sind, so ist ihr Product MM' ebenfalls durch Φ darstellbar. Bedeuten überhaupt M, M', M'', etc. eine Reihe von ganzen, durch die Form Φ darstellbaren Zahlen, so giebt es in dem Ausdrucke

$$M^m M'^{m'} M''^{m''} \ldots,$$

in welchem die Exponenten die Null und alle positiven ganzen Zahlen vorstellen, unendlich viele ganze Zahlen, welche durch die Form Φ dargestellt werden können.

Dies ist ungefähr Alles, was sich bei der Erforschung der Eigenschaften der Formen Φ gewissermafsen an der Oberfläche darbietet. Indem wir uns nun zu schwierigeren und tiefer liegenden Untersuchungen wenden, beginnen wir mit derjenigen über die Natur der Theiler der durch die Form Φ darstellbaren Zahlen.

Es heifse eine ganze Zahl q *Theiler der Form*

$$\Phi = u^3 + pp_1(v+w\varrho)^3 + pp_2(v+w\varrho^2)^3 - 3pu(v+w\varrho)(v+w\varrho^2),$$

wenn eine Zahl M existirt, in die q aufgeht und welche durch die Form Φ darstellbar ist, ohne dafs die Variabeln u, v, w einen gemeinschaftlichen Theiler hätten; diese letztere Bedingung ist darum nothwendig, weil sonst das Characteristische der Theiler verloren ginge und jede Zahl Theiler der Form Φ sein könnte. Im entgegengesetzten Falle, d. h. wenn keine solche Zahl M existirt, die durch Φ in relativen Primzahlen darstellbar und $\equiv 0$ (mod. q) ist, heifse q *Nichttheiler* der Form Φ.

Wenn eine ganze Zahl Theiler der Form Φ ist, so ist, wie man sogleich sieht, jeder ihrer Primfactoren ebenfalls ein Theiler der Form Φ. Wir wollen also zuerst alle Primzahlen aufsuchen, welche Theiler dieser Form sein können.

Es sei q eine reelle positive Primzahl, für welche $\Phi \equiv 0 \pmod{q}$ ist, während u, v, w relative Primzahlen, d. h. nicht alle drei durch ein und dieselbe Zahl theilbar sind; wir setzen q von 3 und von p verschieden voraus, weil $q=3$, $q=p$ immer Theiler von Φ sind. Sehen wir nun, welche Folgerungen sich aus einer solchen Annahme ziehen lassen. Setzt man $v+w\varrho=y$, $v+w\varrho^2=z$, so können auch u, y, z keinen gemeinschaftlichen Factor haben; aufser vielleicht den Factor $1-\varrho$: diese letzteren Variabeln können also nicht alle drei mit q denselben gemeinschaftlichen Theiler haben; aber auch nicht zwei von ihnen, weil sonst vermittelst der Congruenz $\Phi \equiv 0 \pmod{q}$ Dasselbe auch für den dritten gelten würde. Es sei δ entweder $=q$, wenn q von der Form $3n+2$, oder δ gleich einem der beiden complexen Primfactoren q_1 von q, wenn $q=3n+1$ ist. Es sind nun zwei Fälle denkbar: entweder ist eine der drei Variabeln u, y, z durch δ theilbar, oder sie sind alle drei *nicht* durch δ theilbar. Es sei u durch δ theilbar; dann sind y und z nicht durch δ theilbar, und man kann statt $\Phi \equiv 0 \pmod{\delta}$ einfacher $pp_1y^3+pp_2z^3 \equiv 0 \pmod{\delta}$ schreiben. Dies giebt

$$\left[\frac{pp_1y^3}{\delta}\right]=\left[\frac{-pp_2z^3}{\delta}\right], \qquad \left[\frac{pp_1}{\delta}\right]=\left[\frac{pp_2}{\delta}\right],$$

$$\left[\frac{pp_1}{\delta}\right]^2=\left[\frac{p^2}{\delta}\right]=1, \quad \left[\frac{pp_2}{\delta}\right]^2=\left[\frac{p^2}{\delta}\right]=1, \text{ folglich } \left[\frac{pp_1}{\delta}\right]=\left[\frac{pp_2}{\delta}\right]=1.$$

Dasselbe Resultat erhält man, wenn y oder z durch δ theilbar ist; denn in diesem Falle hat man entweder $u^3+pp_2z^3 \equiv 0$, oder $u^3+pp_1y^3 \equiv 0 \pmod{\delta}$, folglich resp. $\left[\frac{pp_2}{\delta}\right]=1$ oder $\left[\frac{pp_1}{\delta}\right]=1$; und von diesen beiden letztern Gleichungen ist jede eine Folge der andern.

Es bleibt der Fall zu betrachten, wenn u, y, z alle drei nicht durch δ theilbar sind. In diesem Falle setze man

$$\Phi' = u'^3+pp_1y'^3+pp_2z'^3-3pu'y'z',$$

und suche die *complexen* ganzen Zahlen u', y', z' so zu bestimmen, dafs das Product

$$\Phi\Phi' = \mathfrak{u}^3+pp_1\mathfrak{y}^3+pp_2\mathfrak{z}^3-3p\mathfrak{u}\mathfrak{y}\mathfrak{z}$$

die einfachste Gestalt annimmt. Die Werthe von $\mathfrak{u}, \mathfrak{y}, \mathfrak{z}$ sind

$$\mathfrak{u}=uu'+pyz'+pzy', \quad \mathfrak{y}=uy'+yu'+p_2zz', \quad \mathfrak{z}=uz'+zu'+p_1yy'.$$

Es lassen sich nun zwei Wege einschlagen, indem man entweder $\mathfrak{z}=0$ oder $\mathfrak{y}=0$ setzt: welcher von beiden in jedem Falle vorzuziehen sei, wird sogleich die Rechnung zeigen. Setzt man $\mathfrak{z}=0$, so hat man die beiden Gleichungen

$$uy'+yu' = -p_2zz'+\mathfrak{y}, \qquad p_1yy'+zu' = -uz',$$

welche, nach y' und u' aufgelöset,

$$(uz-p_1y^2)y' = (uy-p_2z^2)z'+z\mathfrak{y} \text{ und}$$
$$(uz-p_1y^2)u' = (pyz-u^2)z'-p_1y\mathfrak{y}$$

geben. Ist nun die Determinante $uz-p_1y^2$ nicht durch δ theilbar, so setze man $z'=\mathfrak{y}=uz-p_1y^2$, und man wird für y' und u' *ganze* Werthe aus obigen Gleichungen erhalten, und $\mathfrak{y}$ wird nicht durch δ theilbar sein; man kann also dann Φ' so bestimmen, dafs $\mathfrak{z}=0$ und $\mathfrak{y}$ nicht durch δ theilbar sind; da aber $\Phi\Phi'\equiv 0 \pmod{\delta}$ ist, so hat man $\mathfrak{u}^3+pp_1\mathfrak{y}^3\equiv 0 \pmod{\delta}$, folglich $\left[\frac{pp_1}{\delta}\right]=1$.

Ist aber $uz-p_1y^2$ durch δ theilbar, so mufs man auf dieses System von Gleichungen ganz verzichten und mufs $\mathfrak{y}=0$ setzen; diese Annahme liefert $(uy-p_2z^2)z'=(uz-p_1y^2)y'+y\mathfrak{z}$, $(uy-p_2z^2)u'=(pyz-u^2)y'-p_2z\mathfrak{z}$. Ist nun $uy-p_2z^2$ nicht durch δ theilbar, so darf man nur $y'=\mathfrak{z}=uy-p_2z^2$ setzen, und man wird z', u' in ganzen Zahlen, $\mathfrak{z}$ *nicht* durch δ theilbar, und $\mathfrak{u}^3+pp_2\mathfrak{z}^3\equiv 0 \pmod{\delta}$ erhalten; letztere Congruenz liefert folglich $\left[\frac{pp_2}{\delta}\right]=1$.

Wenn aber zu gleicher Zeit die beiden Congruenzen

$$uz-p_1y^2 \equiv 0, \quad uy-p_2z^2 \equiv 0 \pmod{\delta}$$

Statt finden, so führt gerade die Verbindung dieser beiden Congruenzen zu derjenigen Folgerung, welche dieselben auf anderem Wege zu ziehen nicht erlauben. In der That: multiplicirt man die erste mit $2py$, die zweite mit pz und addirt, so erhält man

$$3puyz-pp_1y^3-pp_2z^3-pp_1y^3\equiv 0 \pmod{\delta}, \quad \text{oder} \quad u^3-pp_1y^3-\Phi\equiv 0;$$

aber $\Phi\equiv 0 \pmod{\delta}$, folglich $u^3\equiv pp_1y^3 \pmod{\delta}$; und da nun y nicht durch δ theilbar ist, so folgt $\left[\frac{pp_1}{\delta}\right]=1$.

Man sieht also, dafs in allen Fällen die beiden Gleichungen

$$(6.) \quad \left[\frac{pp_1}{\delta}\right]=1, \quad \left[\frac{pp_2}{\delta}\right]=1,$$

von denen jede eine unmittelbare Folge der andern ist, die nothwendige Bedingung enthalten, damit q ein Theiler von Φ sei. Ich behaupte, dafs diese Bedingung auch hinreichend ist. In der That, wenn die beiden Gleichungen (6.) erfüllt sind, so giebt es zwei reelle ganze Zahlen α und β von der Art, dafs $\alpha+\beta\varrho^2$ zu p relative Primzahl ist und dafs $(\alpha+\beta\varrho^2)^3\equiv pp_1 \pmod{\delta}$, oder dafs

$$(\alpha+\beta\varrho^2-\eta)(\alpha+\beta\varrho^2-\varrho\eta)(\alpha+\beta\varrho^2-\varrho^2\eta)$$

durch δ theilbar ist; die Norm dieses Ausdrucks wird also durch q theilbar

sein. Die Norm des ersten Factors ist $= (\alpha+\beta\varrho^2-\eta)(\alpha+\beta\varrho-\vartheta) = \alpha^2-\alpha\beta+\beta^2-p-(\alpha+\beta\varrho)\eta-(\alpha+\beta\varrho^2)\vartheta$, und die Normen der beiden andern Factoren werden hieraus erhalten, wenn man statt η, ϑ resp. $\varrho\eta$, $\varrho^2\vartheta$; $\varrho^2\eta$, $\varrho\vartheta$ schreibt. Das Product dieser drei Normen, d. h. die Norm des ganzen obigen Ausdrucks, erscheint also in der Form Φ, und Φ ist somit durch q theilbar. Es bleibt noch zu zeigen, dafs die Variabeln $u=\alpha^2-\alpha\beta+\beta^2-p$, $v=-\alpha$, $w=-\beta$ keinen gemeinschaftlichen Theiler haben: ein solcher gemeinschaftlicher Theiler müfste auch p theilen, also auch $\alpha+\beta\varrho^2$ und p; was gegen die Annahme ist.

Wir kommen jetzt zu der Umformung der Gleichungen (6.) mit Hülfe des Reciprocitätsgesetzes für die cubischen Reste, welches wir im 27ten Bande dieses Journals (Seite 289) bewiesen haben. Wenn zuerst $q=3n+2$ und $\delta=q$ ist, so hat man $\left[\frac{pp_1}{q}\right]=\left[\frac{q}{p_1}\right]$ (Vergl. a. a. O. Seite 305). Wenn zweitens $q=3n+1=q_1q_2$ und $\delta=q_1$ ist, so hat man $\left[\frac{pp_1}{q_1}\right]=\left[\frac{q}{p_1}\right]$ (a. a. O. Seite 307 (α.)). In allen Fällen lassen sich also die Bedingungen (6.) durch die folgende ersetzen:

$$(7.)\quad \left[\frac{q}{p_1}\right]=1.$$

Wenn die Bedingung (7.) erfüllt ist, so ist q cubischer Rest zu p_1, d. h. es existirt ein Cubus λ^3 (welcher immer reell angenommen werden darf), der $\equiv q \pmod{p_1}$ ist. Der *reelle* Ausdruck λ^3-q kann aber nicht anders durch p_1 theilbar sein, als wenn derselbe auch durch p theilbar ist: folglich ist q cubischer Rest zu p. Folgendes ist also das Resultat der Untersuchung:

Lehrsatz 3.

„*Alle Primzahlen q, welche zu p cubische Reste sind* (in der reellen Theorie), *und nur diese, können Theiler der Form Φ sein; die nichtcubischen Reste sind die Nichttheiler.*"

Wenn also irgend eine zusammengesetzte Zahl M, welche relative Primzahl zu $3p$ ist, Theiler der Form Φ ist, so müssen nothwendig ihre sämmtlichen Primfactoren cubische Reste zu p sein. Es ist leicht, mit Hülfe der bis jetzt benutzten Principien zu beweisen, dafs diese Bedingung auch hinreichend ist, und dafs die Formel

$$q^\alpha q'^\beta q''^\gamma \ldots.$$

in der That alle Theiler der Form Φ darstellt (die zu $3p$ relative Primzahlen sind), wenn q, q', q'', ... alle möglichen Primzahlen vorstellen, welche

cubische Reste zu p sind; was jedoch der Kürze halber dem Leser überlassen bleibt.

Das eben ausgesprochene Resultat enthält die wichtige Wahrheit, dafs, ebenso wie bei den quadratischen Formen $x^2 \pm py^2$, auch alle Primtheiler der Form Φ in einer bestimmten Anzahl, nämlich $\frac{1}{3}(p-1)$, *linearer Formen* enthalten sind. Nach Anleitung unseres Satzes haben wir nachstehende kleine Tabelle für die Primtheiler der Formen Φ construirt.

Primtheiler der Form dritten Grades $u^3 + pp_1 y^3 + pp_2 z^3 - 3puyz = \Phi$, wo $y = v + w\varrho$, $z = v + w\varrho^2$ ist und u, v, w reelle ganze Zahlen sind.

$p =$	$p_1 =$	$p_2 =$	Formen der Primtheiler von Φ.
7	$2+3\varrho$	$2+3\varrho^2$	$7n \pm 1$.
13	$-1+3\varrho$	$-1+3\varrho^2$	$13n \pm 1$, ± 5.
19	$5+3\varrho$	$5+3\varrho^2$	$19n \pm 1$, ± 7, ± 8.
31	$5+6\varrho$	$5+6\varrho^2$	$31n \pm 1$, ± 2, ± 4, ± 8, 15.
37	$-4+3\varrho$	$-4+3\varrho^2$	$37n \pm 1$, ± 6, ± 8, ± 10, ± 11, ± 14.
43	$-1+6\varrho$	$-1+6\varrho^2$	$43n \pm 1$, ± 2, ± 4, ± 8, ± 11, ± 16, ± 21.
61	$5+9\varrho$	$5+9\varrho^2$	$61n \pm 1$, ± 3, ± 8, ± 9, ± 11, ± 20, ± 23, ± 24, ± 27, ± 28.
67	$2+9\varrho$	$2+9\varrho^2$	$67n \pm 1$, ± 3, ± 5, ± 8, ± 9, ± 14, ± 15, ± 22, ± 24, ± 25, ± 27.
73	$8+9\varrho$	$8+9\varrho^2$	$73n \pm 1$, ± 3, ± 7, ± 8, ± 9, ± 10, ± 17, ± 21, ± 22, ± 24, ± 27, ± 30.
79	$-7+3\varrho$	$-7+3\varrho^2$	$79n \pm 1$, ± 8, ± 10, ± 12, ± 14, ± 15, ± 17, ± 18, ± 21, ± 22, ± 27, ± 33, ± 38.
97	$11+3\varrho$	$11+3\varrho^2$	$97n \pm 1$, ± 8, ± 12, ± 18, ± 19, ± 20, ± 22, ± 27, ± 28, ± 30, ± 33, ± 34, ± 42, ± 45, ± 46, ± 47.

§. 4.

Theorie der Gleichung $\Phi = 1$.

Da die Theorie der unbestimmten Gleichung $\Phi = 1$ für das Folgende von grofser Wichtigkeit ist, und da sich dieselbe unmittelbar an das im §. 2. Gesagte anschliefst, so wollen wir in diesem Paragraphen zuerst zeigen, dafs diese Gleichung immer ganze Lösungen u, v, w hat, für welche die drei linearen Factoren von Φ irrational sind, und sodann das gemeinsame Band aufsuchen, welches alle ihre unendlich vielen Lösungen verknüpft.

I. Zunächst werde bemerkt, dafs, wenn man der Kürze halber

$$u+(v+w\varrho)\eta+(v+w\varrho^2)\vartheta = \psi(u,v,w),$$
$$u+(v+w\varrho)\varrho\eta+(v+w\varrho^2)\varrho^2\vartheta = \psi'(u,v,w),$$
$$u+(v+w\varrho)\varrho^2\eta+(v+w\varrho^2)\varrho\vartheta = \psi''(u,v,w)$$

setzt, zwei Ausdrücke wie $\psi(u,v,w)$, $\psi(u',v',w')$, in denen die Variabeln als *ganze* oder auch nur als *rationale* Zahlen vorausgesetzt werden, nur dann einander gleich sein können, wenn $u=u'$, $v=v'$, $w=w'$ ist. Um dies zu beweisen, haben wir zu zeigen, dafs aus der Annahme $\psi(u,v,w)=0$ nothwendig $u=v=w=0$ folgt. Wäre dies letztere nicht der Fall, so würden die beiden algebraischen Gleichungen nach η

$$u+(v+w\varrho)\eta+\frac{v+w\varrho^2}{p_1}\eta^2 = 0 \quad \text{und} \quad \eta^3-pp_1 = 0,$$

mit rationalen complexen Coëfficienten, eine gemeinschaftliche Wurzel $\eta=\sqrt[3]{(pp_1)}$ haben. Daraus würde vermittelst der Operation des gröfsten gemeinschaftlichen Theilers weiter folgen, dafs $\sqrt[3]{(pp_1)}$ einer rationalen complexen Zahl gleich sein müfste: also müfste pp_1 ein rationaler Cubus, folglich als ganze Zahl ein ganzer (complexer) Cubus sein; was ungereimt ist, da in $pp_1=p_1^2p_2$ nicht die Exponenten der complexen Primfactoren durch 3 theilbar sind. Aus der Annahme $\psi(u,v,w)=\psi(u',v',w')$ folgt aber $\psi(u-u',\ v-v',\ w-w')=0$, folglich $u-u'=0$, $v-v'=0$, $w-w'=0$; was zu beweisen war. Natürlich gilt derselbe Satz auch in Beziehung auf die beiden andern linearen Ausdrücke ψ' und ψ''. Übrigens lassen sich ψ' und ψ'' immer auf die Form ψ bringen; denn es ist, wie man sieht,

$$\psi'(u,v,w) = \psi(u,-w,v-w),$$
$$\psi''(u,v,w) = \psi(u,w-v,-v).$$

Da diese letztere Umformung so einfach ist, so wird sie später immer stillschweigend vorausgesetzt werden. Wenn also der Werth von ψ gegeben ist, so sind dadurch die *rationalen* Zahlen u, v, w vollkommen bestimmt, und durch ψ sind auch ψ', ψ'' vollkommen mitgegeben; vorausgesetzt, dafs einem solchen Werthe von ψ in der That rationale Werthe von u, v, w entsprechen: denn dafs man dem Ausdrucke ψ unendlich viele Werthe ertheilen kann, für welche u, v, w auf keine Weise rational bestimmt werden können, leidet keinen Zweifel. Es folgt auch hieraus, dafs ψ nur dann einen *rationalen* Werth erhalten kann, wenn v und w verschwinden; und dieser rationale Werth ist dann immer $=u$. In Beziehung auf die Gleichung $\Phi=1$ ist folglich $u=1$, $v=0$, $w=0$ die einzige Lösung, für welche ψ einen rationalen Werth erhält; für alle übrigen

Lösungen, so viele es deren auch geben mag, sind ψ, ψ', ψ'' alle drei irrational, und v, w können nicht beide zugleich verschwinden. Es ist gut, hier sogleich zu bemerken, dafs für reelle Werthe u, v, w die drei linearen Factoren ψ, ψ', ψ'' von Φ immer reelle Werthe annehmen, und dafs, wenn die Gleichung $\Phi = 1$ erfüllt wird, nur entweder alle drei positiv, oder einer positiv, die beiden andern negativ sein können.

II. Wir haben in §. 2. gesehen, dafs sich die ganze Function $27\frac{x^p-1}{x-1}$ auf die Form

$$(1.)\quad 27(x^{p-1}+x^{p-2}+\ldots+x+1)$$
$$= U^3+pp_1(V+W\varrho)^3+pp_2(V+W\varrho^2)^3-3pU(V+W\varrho)(V+W\varrho^2)$$
$$= \psi(U,V,W)\psi'(U,V,W)\psi''(U,V,W)$$

bringen läfst, wo U, V, W ganze Functionen von x mit ganzen reellen Coëfficienten sind. Substituirt man in der Gleichung (1.) $x=1$, so erhält man links $27p$; die Polynome U, V, W gehen in reelle ganze Zahlen über, die wir resp. durch U_1, V_1, W_1 bezeichnen, und man erhält

$$(2.)\quad 27p = \psi_1\psi'_1\psi''_1;$$

wo der Kürze wegen ψ_1 u. s. w. statt $\psi(U_1, V_1, W_1)$ u. s. w. gesetzt ist. Der Ausdruck ψ_1 ist nothwendig *irrational:* denn wäre ψ_1 rational, so hätte man nach dem in der vorigen Nummer Bewiesenen $\psi_1 = U_1$ und auch $\psi'_1=\psi''_1=U_1$, folglich $27p = U_1^3$; was ungereimt ist, da p eine Primzahl, folglich $27p$ keinem Cubus gleich sein kann. Die ganze Zahl U_1 ist nothwendig durch p theilbar, wie man aus der Gleichung

$$27p = U_1^3+pp_1Y_1^3+pp_2Z_1^3-3pU_1Y_1Z_1$$

ersieht, wo $Y_1 = V_1+W_1\varrho$, $Z_1 = V_1+W_1\varrho^2$ gesetzt ist. Dividirt man daher jeden der drei Factoren ψ_1, ψ'_1, ψ''_1 durch $\sqrt[3]{p}$, so erhält man die Zahl 27 durch eine cubische Form dargestellt, welche sich in das Product aus drei linearen Factoren zerfällen läfst, von denen der erste folgender ist:

$$T_1\sqrt[3]{p^2}+Y_1\sqrt[3]{p_1}+Z_1\sqrt[3]{p_2},$$

wo $U_1 = pT_1$; während die andern beiden hieraus hervorgehen, wenn man statt der beiden Cubikwurzeln $\sqrt[3]{p_1}$, $\sqrt[3]{p_2}$ ihre übrigen Werthe setzt, immer mit der Beschränkung, dafs das Product beider reell sein mufs. Erhebt man den eben geschriebenen Ausdruck zum *Cubus,* so erhält man einen Ausdruck von der Form

$$3\psi(u, v, w),$$

wo

$$u = \tfrac{1}{3}(p^2T_1^3+p_1Y_1^3+p_2Z_1^3+6pT_1Y_1Z_1),$$
$$v+w\varrho = y = pT_1^2Y_1+p_1T_1Z_1^2+Y_1^2Z_1,$$
$$v+w\varrho^2 = z = pT_1^2Z_1+p_1T_1Y_1^2+Y_1Z_1^2$$

gesetzt ist; erhebt man auf dieselbe Weise die beiden andern linearen Factoren zum Cubus, so erhält man $3\psi'(u,v,w)$, $3\psi''(u,v,w)$. Dafs u eine ganze Zahl ist, ergiebt sich daraus, dafs $p^2T_1^3+p_1Y_1^3+p_2Z_1^3-3T_1Y_1Z_1 = 27$, folglich $u = \frac{1}{3}(27+(3+6p)T_1Y_1Z_1)$ ist. Ich behaupte jetzt, dafs u, v und w durch 3 theilbar sind. Um dies zuerst für v und w zu beweisen, oder, was dasselbe ist, für y und z, bemerke man zunächst, dafs aus den Congruenzen $p^2T_1^3+p_1Y_1^3+p_2Z_1^3 \equiv 0 \pmod{3}$, $p\equiv 1$, $p_1\equiv p_2\equiv -1$, $T_1^3\equiv T_1$, $Y_1^3\equiv Z_1^3\equiv V_1+W_1 \pmod{3}$ die folgende sich ergiebt: $T_1-2V_1-2W_1 \equiv 0 \pmod{3}$, oder $T_1+V_1+W_1\equiv 0 \pmod{3}$, oder, wie hieraus sogleich folgt, wegen $Y_1+Z_1 = 2V_1-W_1$, $T_1\equiv Y_1+Z_1 \pmod{3}$; von der andern Seite erhält man aus den obigen Ausdrückeu für y und z

$$y\equiv T_1^2Y_1-T_1Z_1^2+Y_1^2Z_1,\quad z\equiv T_1^2Z_1-T_1Y_1^2+Y_1Z_1^2 \pmod{3}.$$

Substituirt man nun in diesen Ausdrücken für T_1, $T_1\equiv Y_1+Z_1 \pmod{3}$, so erhält man die folgenden:

$$Y_1^3+3Y_1^2Z_1-Z_1^3,\quad Z_1^3+3Y_1Z_1^2-Y_1^3.$$

Da nun $Y_1^3\equiv Z_1^3 \pmod{3}$ ist, so sieht man, dafs in der That y und z, also auch v und w, durch 3 theilbar sind. Um dasselbe für u nachzuweisen, bemerke man, dafs

$$u^3 = 27^2-pp_1y^3-pp_2z^3+3upyz$$

ist; alle Glieder auf der rechten Seite sind hier durch 27 theilbar, folglich ist auch u^3 durch 27, mithin u durch 3 theilbar. Es sind also $\frac{1}{3}u$, $\frac{1}{3}v$, $\frac{1}{3}w$ ganze Zahlen und geben eine Lösung der Gleichung $\Phi = 27$. Um nicht zu viel neue Buchstaben einzuführen, seien diese drei ganzen Zahlen wiederum blofs durch u, v, w bezeichnet.

Wir wollen jetzt zeigen, wie man durch Cubirung aus dieser Lösung eine neue Lösung der Gleichung $\Phi = 27$ ableiten kann. Erhebt man den Ausdruck $\psi(u,v,w)$ zum Cubus, so erhält man wiederum einen Ausdruck von der Form ψ, für welchen $\psi\psi'\psi'' = 27^3$ ist; ich behaupte, dafs die neuen Variabeln alle drei durch 9 theilbar sind, so dafs man durch $9.9.9 = 27^2$ dividiren kann und in der That eine neue Lösung der Gleichung $\Phi = 27$ erhält. Nachdem diese Behauptung bewiesen ist, erhellet, dafs man auf diese Weise fortfahren und immer aufs Neue aus jeder bereits gefundenen Lösung

durch Cubirung eine neue, also unendlich viele Lösungen der Gleichung $\Phi = 27$ ableiten kann. Die Werthe der neuen Variabeln sind in den Formeln

$$u' = u^3 + pp_1y^3 + pp_2z^3 + 6puyz = 27 + 9puyz,$$
$$y' = v' + w'\varrho = 3(u^2y + p_2uz^2 + py^2z),$$
$$z' = v' + w'\varrho^2 = 3(u^2z + p_1uy^2 + pyz^2)$$

enthalten. In Bezug auf u' ist also nichts zu beweisen, und von y' und z' sieht man wenigstens, dafs sie den Factor 3 enthalten. Es bleibt noch zu zeigen, dafs $\frac{1}{3}y' \equiv \frac{1}{3}z' \equiv 0 \pmod{3}$ ist. Hiervon überzeugt man sich aber sogleich, wenn man die Congruenzen $p \equiv 1$, $p_1 \equiv p_2 \equiv -1 \pmod{3}$, $u^3 \equiv u$, $y^3 \equiv z^3 \equiv v + w \pmod{3}$ und die aus ihrer Verbindung mit der Gleichung $\Phi = 27$ folgende Congruenz $u \equiv y + z \pmod{3}$ zu Hülfe nimmt und dieselben in den Formeln für $\frac{1}{3}y'$ und $\frac{1}{3}z'$ substituirt; die obige Behauptung ist also aufser Zweifel gestellt. Die zuletzt angedeutete Rechnung ist übrigens der schon oben ausgeführten ganz ähnlich, und eine Wiederholung daher überflüssig.

Alle Lösungen der Gleichung $\Phi = 27$, welche man auf diese Weise durch fortgesetzte Cubirung eine aus der andern ableiten kann, sind in der Formel

$$(3.)\qquad u + y\eta + z\vartheta = 3\left(\frac{U_1 + Y_1\eta + Z_1\vartheta}{3\sqrt[3]{p}}\right)^{3^n}$$

enthalten, wo U_1, Y_1, Z_1 dieselbe Bedeutung haben wie oben; nämlich die Werthe der Polynome U, Y, Z aus §. 2. für $x = 1$, während n, der Exponent vom Exponenten 3, alle ganzen positiven Werthe durchläuft. Diese Formel liefert, wie aus dem Bewiesenen erhellet, immer ganze Werthe für u, $y = v + w\varrho$, $z = v + w\varrho^2$, also auch für v und w. Natürlich mufs man bei der Anwendung dieser Formel, wie immer bei Formeln solcher Gattung mit irrationalen Ausdrücken, je zwei entsprechende Glieder mit einander vergleichen, so dafs die Formel implicite *drei* Gleichungen darstellt; auch mufs man sich hierbei der Gleichungen $\eta^3 = pp_1$, $\vartheta^3 = pp_2$, $\eta\vartheta = p$, $\eta^2 = p_1\vartheta$, $\vartheta^2 = p_2\eta$ erinnern, welche bewirken, dafs jede Entwicklung dieser Art sich immer auf drei und nicht mehr wesentlich verschiedene Glieder reducirt.

Es bleibt noch zu zeigen, dafs alle in der Formel (3.) enthaltenen Lösungen der Gleichung $\Phi = 27$ von einander verschieden sind. Zu dem Ende ist nur zu beweisen, dafs der Ausdruck $\frac{U_1 + Y_1\eta + Z_1\vartheta}{3\sqrt[3]{p}}$, welcher immer reell ist, einen von der *Einheit* verschiedenen Werth hat; denn verschiedene Potenzen eines reellen und von der Einheit verschiedenen Ausdrucks sind

immer verschieden. Es seien der Kürze wegen $U_1+Y_1\eta+Z_1\vartheta=A$, und B, C seien die *correspondirenden* *) Ausdrücke von A. Wäre nun, gegen die Voraussetzung, $A=3\sqrt[3]{p}$, so wäre auch $A^3=27p$; von der andern Seite ist ABC ebenfalls $=27p$ (2.), also $A^2=BC$, folglich auch $B^2=AC$, $C^2=AB$; welches die correspondirenden Relationen sind. Hieraus folgt

$$A^4=B^2C^2=AC^3, \qquad A^8=A^2C^6=A^5B^3,$$

mithin $A^3=B^3$. Da aber A und B reell sind, so giebt dies $A=B$, folglich, wegen $A^2=BC$, auch $A=C$. Addirt man die drei Gleichungen $A=A$, $A=B$, $A=C$, so erhält man $3A=3U_1$, $A=U_1$, folglich wäre A rational; gegen das oben Bewiesene. Die Formel (8.) giebt also in der That lauter verschiedene Lösungen.

III. Es wurde in der vorigen Nummer gezeigt, dafs die Gleichung $\Phi=27$ immer unendlich viele Lösungen hat. Sehen wir jetzt, wie sich Lösungen der Gleichungen $\Phi=1$ aus jenen ableiten lassen. Wir nennen der Kürze halber zwei complexe Ausdrücke, wie $u+y\eta+z\vartheta$, $u'+y'\eta+z'\vartheta$, nach dem Modul μ congruent, wenn zu gleicher Zeit die drei Congruenzen $u\equiv u'$, $y\equiv y'$, $z\equiv z'$ (mod. μ) erfüllt sind; im entgegengesetzten Falle heifsen sie incongruent. Da es, wenn der Modul $=27$ gesetzt wird, nur 27^3 nach demselben incongruente complexe Ausdrücke geben kann, so werden sich unter je 27^3+1 solchen Ausdrücken wenigstens zwei congruente befinden. Entlehnt man also der Formel (3.), welche unendlich viele verschiedene Lösungen der Gleichung $\Phi=27$ giebt, nur 27^3+1 solche Lösungen, so folgt, dafs sich unter denselben gewifs zwei congruente $P\equiv Q$ (mod. 27) befinden werden. Es seien P', P'' die zu P und Q', Q'' die zu Q correspondirenden Ausdrücke; dann wird man, wenn man die eben geschriebene Congruenz auf beiden Seiten mit $Q'Q''$ multiplicirt,

$$PQ'Q''\equiv QQ'Q'' \text{ (mod. 27)}$$

haben. Aber $QQ'Q''=27$, folglich $PQ'Q''\equiv 0$ (mod. 27); also sind in dem Ausdrucke $PQ'Q''$ die drei Variabeln durch 27 theilbar; man erhält

---

*) Die correspondirenden Ausdrücke eines Ausdrucks von der Form $u+y\eta+z\vartheta$ mögen ein für allemal die Ausdrücke $u+y\varrho\eta+z\varrho^2\vartheta$, $u+y\varrho^2\eta+z\varrho\vartheta$ genannt werden, welche aus jenen entstehen, wenn man statt der Cubikwurzeln η, ϑ die andern einführt, deren Product ebenfalls reell und $=p$ ist. Es ist zu bemerken, dafs, wenn A, B, C, ebenso wie A', B', C', correspondirende Ausdrücke sind und $A=A'$ ist, daraus nothwendig $B=B'$, $C=C'$ folgt; wie unmittelbar aus (1.) folgt, vorausgesetzt, dafs die Variabeln rational sind, wie dies auch in gegenwärtigen Untersuchungen nie anders der Fall ist. Diese beiden abgeleiteten Relationen heifsen die *correspondirenden* Relationen.

mithin, wenn man durch 27 dividirt, in dem Ausdrucke

$$\frac{PQ'Q''}{27} = u+y\eta+z\vartheta = \frac{P}{Q}$$

eine Lösung der Gleichung $\Phi = 1$. In der That ist u eine reelle ganze Zahl, y, z sind conjugirte complexe ganze Zahlen, und von der andern Seite sind die correspondirenden Ausdrücke von $\frac{PQ'Q''}{27}$ die folgenden: $\frac{P'Q''Q}{27}$, $\frac{P''QQ'}{27}$, und das Product aller drei ist $= \frac{PP'P''.QQ'Q''.QQ'Q''}{27^3} = 1$; wie zu beweisen war. Aber diese Lösung ist auch nothwendig irrational; denn wäre es anders, so müfste man $\frac{PQ'Q''}{27} = 1$ haben, d. h. $\frac{P}{Q} = 1$, $P = Q$, und die beiden Lösungen P und Q wären nicht verschieden, wie doch angenommen wurde.

IV. Nachdem man sich auf diese Weise überzeugt hat, dafs die Gleichung $\Phi = 1$ immer in ganzen reellen Zahlen u, v, w lösbar ist, für welche die drei linearen Factoren von Φ irrationale Werthe annehmen, kommt man zu der weit schwierigeren Untersuchung, welche die wirkliche Angabe aller Lösungen und die passende Anordnung unter denselben betrifft. Die *Pell*sche Gleichung bietet bis jetzt das einzige Beispiel einer solchen Anordnung von unendlich vielen Lösungen dar; aber unsere Gleichung, wiewohl in mehreren Puncten jener sehr ähnlich, zeigt in dieser Hinsicht so wenig Analogie, dafs es mir, trotz der, wie man sehen wird, grofsen Einfachheit und Eleganz des Resultats, erst nach vielen mühsamen Versuchen gelungen ist, das Gesetz zu entdecken.

Wenn u, v, w irgend eine Lösung der Gleichung $\Phi = 1$ ist, für welche der erste Linearfactor $A = u+(v+w\varrho)\eta+(v+w\varrho^2)\vartheta$ einen irrationalen Werth hat, und B, C die dem A correspondirenden Factoren sind, so behaupte ich, dafs nie irgend eine ganze Potenz von A irgend einer ganzen Potenz von B gleich sein kann, d. h., dafs die Gleichung $A^m = B^n$ nie durch irgend welche positive oder negative ganze Werthe von m und n ($m = n = 0$ ausgeschlossen) erfüllt werden kann. Denn existirte wirklich, gegen die Behauptung, eine Gleichung von dieser Form, so sind nur zwei Fälle denkbar. Entweder man hat $m = n$, also $A^m = B^m$, folglich auch die correspondirenden Relationen $B^m = C^m$, $C^m = A^m$, d. h. $A^m = B^m = C^m$; da man aber auch $A^m B^m C^m = 1$ hat, so würde hieraus $A^m = 1$, $A = 1$ folgen, und A gegen die Voraussetzung irrational. Oder m und n sind verschieden; aus $A^m = B^n$ folgen die correspondirenden Relationen $B^m = C^n$, $C^m = A^n$; erhebt man die

erste dieser drei Gleichungen zur Potenz m^2, und benutzt die zweite und dritte, so erhält man

$$A^{m^3} = B^{m^2 n} = C^{mn^2} = A^{n^3}, \quad \text{also} \quad A^{m^3} = A^{n^3};$$

was offenbar unmöglich ist, da A reell und von der Einheit verschieden ist, also zwei verschiedene Potenzen von A, nämlich die m^3te und n^3te nicht einander gleich sein können. Da beide Fälle nicht stattfinden können, so ist die Behauptung erwiesen. — Es wird in der Folge häufig die Rede von dem natürlichen Logarithmen des *absoluten* Werthes eines reellen Ausdrucks sein; wir wollen uns zu diesem Behufe des Zeichens Log bedienen, so dafs für irgend einen reellen Werth k, $\operatorname{Log} k = \log k$ ist, wenn k positiv, dagegen $\operatorname{Log} k = \log(-k)$, wenn k negativ ist, oder, wenn man will, in allen Fällen $\operatorname{Log} k = \frac{1}{2}\log(k^2) = \log(+\sqrt{k^2})$. Wir haben schon in (I.) gesehen, dafs jede Lösung u, v, w der Gleichung $\Phi = 1$ durch den Werth von A vollkommen bestimmt ist; sie ist es aber auch durch den Werth von $\operatorname{Log} A$; denn durch $\operatorname{Log} A$ ist A in so weit bestimmt, dafs man nur über das Vorzeichen zweifelhaft sein könnte; jedoch von den beiden Linearfactoren $\pm A$ kann nur einer die Gleichung erfüllen, während der andere, für welchen die Variabeln u, v, w in $-u, -v, -w$ übergehen, die Gleichung $\Phi = -1$ befriedigt, also ist auch das Vorzeichen von A vollkommen bestimmt.

Für alle Lösungen unserer Gleichung, mit Ausnahme der einzigen $u = 1$, $v = w = 0$, ist der Werth von $\frac{\operatorname{Log} A}{\operatorname{Log} B}$ immer nothwendig irrational; denn wäre $\frac{\operatorname{Log} A}{\operatorname{Log} B} = \frac{n}{m}$, wo m und n ganze Zahlen sind, so wäre $m \operatorname{Log} A = n \operatorname{Log} B$, also indem man von den Logarithmen zu den Zahlen übergeht, $(\pm A)^m = (\pm B)^n$ und $A^{2m} = B^{2n}$; gegen das oben Bewiesene, dafs keine Potenz von A einer Potenz von B gleich sein kann. Es folgt hieraus unmittelbar, nach einem bekannten und wichtigen Satze, auf welchen auch *Jacobi* seine Untersuchungen über mehrfache Periodicität gegründet hat, dafs es immer unendlich viele ganze Zahlen m und n giebt, für welche der absolute Werth des Ausdrucks

$$m \operatorname{Log} A + n \operatorname{Log} B = \operatorname{Log} A \left(m \frac{\operatorname{Log} A}{\operatorname{Log} B} + n\right)$$

unter einer beliebig gegebenen, noch so kleinen positiven Grenze ε liegt. Wir können jetzt den Satz beweisen:

Dafs es immer unendlich viele Lösungen unserer Gleichung giebt, für welche der absolute Werth des ersten Linearfactors von Φ der Einheit so nahe kommt, als man will.

In der That: wenn für irgend eine bereits bekannte (irrationale) Lösung unserer Gleichung, A der Werth des ersten Linearfoctors ist, B und C die beiden andern Linearfactoren sind, und man setzt $A' = A^m B^n$, so giebt A' für alle ganzen Werthe von m und n Lösungen unserer Gleichung. Für positive Werthe von m und n ist dies von selbst klar, und für negative Werthe der Exponenten darf man nur $\frac{1}{A}$, $\frac{1}{B}$ resp. durch BC, AC ersetzen. Nun ist $\operatorname{Log} A' = m \operatorname{Log} A + n \operatorname{Log} B$, also kann man über m und n auf unendlich viele Arten so disponiren, dafs der absolute Werth von $\operatorname{Log} A' < \varepsilon$ wird, und folglich kann man für unendlich viele Lösungen den absoluten Werth von $\operatorname{Log} A'$ der Null, mithin den absoluten Werth von A' der Einheit so nahe rücken, als man will.

Hingegen giebt es nur eine endliche Anzahl von Lösungen, oder vielleicht gar keine, für welche zugleich die beiden Bedingungen $\pm \operatorname{Log} A < \varepsilon$, $\pm \operatorname{Log} B < \varepsilon'$ *erfüllt werden, wo* ε *und* ε' *irgend zwei gegebene positive Constanten sind.*

Die Richtigkeit hiervon kann zwar leicht analytisch nachgewiesen werden, indem man Grenzen für die Variabeln u, v, w selbst angiebt, welche den gemachten Bedingungen entsprechen: aber am deutlichsten wird der Gegenstand wenn man eine geometrische Anschauung zu Hülfe nimmt. In der That: wenn man alle Puncte des Raumes durch rechtwinklige Coordinaten u, v, w ausdrückt, und A, B, so wie Φ als Functionen derselben betrachtet, so sieht man durch die einfachsten Sätze der analytischen Geometrie ein, dafs alle Puncte des Raumes, für welche die beiden oben aufgestellten Ungleichheitsbedingungen und die dritte $0 < \Phi \leqq 1$ erfüllt sind, einen vollkommen begrenzten und von allen Seiten eingeschlossenen Körper ausmachen. Theilt man den unendlichen Raum durch gleich weit entfernte Ebenen parallel mit den Axen in lauter gleiche Würfel mit den Dimensionen $=1$, so entsprechen den Eckpuncten dieser Würfel die ganzen Werthe von u, v, w; aber offenbar können innerhalb des endlichen Körpers und auf dem ihn begrenzenden Theil der Oberfläche $\Phi = 1$ nur eine *endliche* Anzahl von Würfeleckpuncten liegen; folglich ist unsere Behauptung aufser Zweifel gestellt.

Folglich giebt es auch nur eine endliche Anzahl von Lösungen, für welche

$$(4.) \qquad N(\operatorname{Log} A - \varrho \operatorname{Log} B) < \varepsilon \textit{ ist *)}.$$

*) Unter der Norm eines complexen Ausdrucks $\mu + \nu i$, $N(\mu + \nu i)$, verstehen wir immer den Ausdruck $(\mu + \nu i)(\mu - \nu i) = \mu^2 + \nu^2$, wenn μ und ν reell sind.

Denn die Bedingung (4.) ist gleichbedeutend mit dieser: $(2\operatorname{Log}A+\operatorname{Log}B)^2+3(\operatorname{Log}B)^2<4\varepsilon$, oder auch mit dieser: $(2\operatorname{Log}B+\operatorname{Log}A)^2+3(\operatorname{Log}A)^2<4\varepsilon$, welche die beiden folgenden nach sich ziehen: $(\operatorname{Log}B)^2<\frac{4}{3}\varepsilon$, $(\operatorname{Log}A)^2<\frac{4}{3}\varepsilon$; so dafs wir auf den vorigen Satz zurückkommen.

Läfst man demnach die positive Constante ε stetig abnehmen, so wird man einmal zu einem so kleinen Werthe von ε gelangen, dafs es durchaus keine irrationale Lösung der Gleichung $\Phi=1$ giebt, für welche die Bedingung (4.) erfüllt ist. Steigt man von einem solchen Werthe von ε wiederum stetig aufwärts, so mufs man einmal zu einer Lösung gelangen, für welche genau $N(\operatorname{Log}A-\varrho\operatorname{Log}B)=\varepsilon$ ist, ohne dafs diesem vollkommen bestimmten Werthe von ε, den wir durch σ bezeichnen, irgend eine andere der Bedingung (4.) genügende Lösung entspricht. Es kann mehrere Lösungen geben, für welche

$$(5.)\qquad N(\operatorname{Log}A-\varrho\operatorname{Log}B)=\sigma$$

ist, aber wenigstens wird man auf diesem Wege überzeugt, dafs es aufser der Lösung $u=1$, $v=w=0$, welche wir immer von der Betrachtung ausschliefsen, keine andere giebt, für welche

$$N(\operatorname{Log}A-\varrho\operatorname{Log}B)<\sigma \text{ wäre.}$$

Alle Lösungen, welche dem *Minimum* von $N(\operatorname{Log}A-\varrho\operatorname{Log}B)$ entsprechen, d. h. welche der Gleichung (5.) genügen, heifsen *Fundamental-Auflösungen* der Gleichung $\Phi=1$.

V. Wenn A, B, C die drei Linearfactoren von Φ sind, welche einer beliebigen, aber bestimmten *Fundamental-Auflösung* entsprechen, so behaupte ich, dafs alle möglichen Lösungen unserer Gleichung in der Formel

$$(6.)\qquad u+(v+w\varrho)\eta+(v+w\varrho^2)\vartheta = A' = A^m B^n$$

enthalten sind; wo m, n alle möglichen positiven und negativen ganzen Zahlen und die Null zu Werthen erhalten müssen.

Erstlich sind in der That alle Werthe von u, v, w, welche die Formel (6.) ergiebt, Lösungen der Gleichung $\Phi=1$; denn einerseits giebt die Formel nur ganze Werthe für die Variabeln, und andrerseits sind die dem A' correspondirenden Linearfactoren

$$B'=B^mC^n,\qquad C'=C^mA^n,$$

folglich ist das Product aller drei

$$A'B'C'=(ABC)^{m+n}=1.$$

Zweitens entsprechen verschiedenen Werthen der Exponenten verschiedene Lösungen; denn aus der Annahme $A^mB^n=A^{m'}B^{n'}$ folgt $A^{m-m'}=B^{n'-n}$,

was nach dem schon in (IV.) Bewiesenen nicht sein kann, aufser wenn $m-m'=0$, $n'-n=0$, also $m=m'$, $n=n'$ ist, d. h. wenn die Exponenten übereinstimmen.

Für alle Lösungen der Formel (6.) hat man

$$A'=A^m B^n, \quad B'=B^m C^n=\frac{B^m}{A^n B^n}=A^{-n}B^{m-n},$$

folglich

$$(7.)\quad \operatorname{Log}A'=m\operatorname{Log}A+n\operatorname{Log}B, \quad \operatorname{Log}B'=-n\operatorname{Log}A+(m-n)\operatorname{Log}B.$$

Aus der Verbindung dieser beiden Gleichungen erhält man die merkwürdige Formel

$$(8.)\quad \operatorname{Log}A'-\varrho\operatorname{Log}B'=(m+n\varrho)(\operatorname{Log}A-\varrho\operatorname{Log}B);$$

alle Werthe von $\operatorname{Log}A'-\varrho\operatorname{Log}B'$ werden also aus dem einzigen $\operatorname{Log}A-\varrho\operatorname{Log}B$, welcher der Fundamental-Auflösung, also dem Minimum entspricht, ***durch Multiplication mit allen möglichen complexen ganzen Zahlen*** $m+n\varrho$ ***gefunden.*** Der Kürze wegen soll für jede Lösung der Ausdruck $\operatorname{Log}A'-\varrho\operatorname{Log}B'$ der ***Regulator*** genannt werden.

Die Gleichung (8.) ist eine nothwendige Folge der Gleichung (6.); aber umgekehrt ist auch (6.) eine nothwendige Folge von (8.); denn da $\operatorname{Log}A'$ und $\operatorname{Log}B'$ reell sind, so zerlegt sich die Gleichung (8.) in *zwei* Gleichungen, welche genau die Gleichungen (7.) sind, von denen wiederum die erste nur eine andere Form der Gleichung (6.) darstellt. Wenn man also, was jetzt noch übrig bleibt, zeigen will, dafs es keine andern Lösungen der Gleichung $\Phi=1$ giebt, als die in (6.) enthaltenen, so läfst sich dieses Problem sogleich auf ein anderes reduciren, welches zu beweisen verlangt, dafs der Regulator jeder Lösung in der Form $(m+n\varrho)(\operatorname{Log}A-\varrho\operatorname{Log}B)$ enthalten sei.

Es seien a, b, c die Linearfactoren, welche irgend einer Lösung entsprechen, die man auf irgend eine Weise gefunden hat. Setzt man

$$a'=aA^m B^n, \quad b'=bB^m C^n, \quad c'=cC^m A^n,$$

so sind a', b', c' die correspondirenden Linearfactoren für ebenso viele neue Lösungen, als man den Exponenten m, n ganze Werthe giebt. Da aus $a'=aA^m B^n$, $b'=bB^m C^n=bA^{-n}B^{m-n}$,

$$\operatorname{Log}a'=\operatorname{Log}a+m\operatorname{Log}A+n\operatorname{Log}B \text{ und}$$
$$\operatorname{Log}b'=\operatorname{Log}b-n\operatorname{Log}A+(m-n)\operatorname{Log}B$$

folgt: so erhält man den Regulator aller dieser neuen Lösungen wie folgt ausgedrückt:

$$\operatorname{Log}a'-\varrho\operatorname{Log}b'=\operatorname{Log}a-\varrho\operatorname{Log}b+(m+n\varrho)(\operatorname{Log}A-\varrho\operatorname{Log}B),$$

welches

$$9.\quad \frac{\operatorname{Log} a' - \rho \operatorname{Log} b'}{\operatorname{Log} A - \rho \operatorname{Log} B} = \frac{\operatorname{Log} a - \rho \operatorname{Log} b}{\operatorname{Log} A - \rho \operatorname{Log} B} + m + n\rho \text{ giebt.}$$

Nun sind zwei Fälle denkbar: entweder ist der Quotient $\frac{\operatorname{Log} a - \rho \operatorname{Log} b}{\operatorname{Log} A - \rho \operatorname{Log} B}$, welchen wir $= \alpha + \beta\rho$ setzen, einer complexen *ganzen* Zahl gleich: oder dies ist nicht der Fall. Der erste Fall entspricht unserer Behauptung. Im zweiten Falle kann man immer die ganzen Zahlen m und n so bestimmen, dafs die absoluten Werthe der beiden reellen Zahlen $\alpha + m$ und $\beta + n$ unter der Grenze $\frac{1}{2}$ liegen; d. h. dafs die absoluten Werthe des reellen Theils sowohl, als des Coëfficienten von ρ in dem Ausdrucke (9.), unter der Grenze $\frac{1}{2}$ liegen, ohne dafs beide Theile Null sein können, weil eben nicht α und β zugleich ganze Zahlen sein sollen. Für solche Werthe von m und n wird die Norm des Ausdrucks (9.) $\leqq \frac{3}{4}$, aber > 0. In diesem zweiten Falle würde es also eine Lösung geben, für welche die Norm des Regulators

$$> 0 \text{ und zugleich } \leqq \tfrac{3}{4} N(\operatorname{Log} A - \rho \operatorname{Log} B) \text{ wäre.}$$

Dies ist aber offenbar unmöglich und widerspricht der Definition der Fundamental-Auflösung, nach welcher sie gerade diejenige sein sollte, für welche die Norm des Regulators ein Minimum ist. Da der zweite Fall nicht Statt finden kann, so ist die Behauptung bewiesen.

Als eine Anwendung des eben gefundenen Resultats, wollen wir alle Fundamental-Auflösungen aufsuchen. Fundamental-Auflösungen sind alle diejenigen, für welche die Norm des Regulators $= \sigma$ ist. Da alle Regulatoren in der Formel $(m + n\rho)(\operatorname{Log} A - \rho \operatorname{Log} B)$ enthalten sind, so ist $N(m + n\rho) N(\operatorname{Log} A - \rho \operatorname{Log} B) = \sigma$ zu setzen; aber $N(\operatorname{Log} A - \rho \operatorname{Log} B)$ ist selbst $= \sigma$, also ist $N(m + n\rho) = 1$ zu setzen; für $m + n\rho$ sind also alle complexe Einheiten zu nehmen; welches die folgenden sechs Systeme von Werthen für m und n giebt: $1, 0;\ 0, 1;\ -1, -1;\ -1, 0;\ 0, -1;\ 1, 1$. Es giebt also genau *sechs* Fundamental-Auflösungen; es sind diejenigen, welchen die folgenden Werthe des ersten Linearfactors von Φ entsprechen:

$$A,\quad B,\quad A^{-1}B^{-1},$$
$$A^{-1},\quad B^{-1},\quad AB;$$

oder, was dasselbe ist, die folgenden:

$$A,\quad B,\quad C,$$
$$\frac{1}{A},\quad \frac{1}{B},\quad \frac{1}{C}.$$

Das Resultat der ganzen Untersuchung läfst sich wie folgt aussprechen:

Lehrsatz 4.

„*Die Gleichung* $\Phi = 1$ *hat immer sechs Fundamental-Auflösun-„gen, von denen je drei durch blofse cyclische Permutation der cor-„respondirenden Linearfactoren A, B, C entstehen, und für welche „die Norm des Regulators* $N(\mathrm{Log}\,A - \varrho\,\mathrm{Log}\,B)$ *zu einem Minimum „*$\sigma > 0$ *gemacht wird. Sind für eine dieser Fundamental-Auf-„lösungen A und B zwei correspondirende Linearfactoren, so giebt „die Formel* $A^m B^n$, *oder die Formel* $(m + n\varrho)(\mathrm{Log}\,A - \varrho\,\mathrm{Log}\,B)$, *alle „Lösungen der Gleichung* $\Phi = 1$."

Es wäre noch übrig, einen einfachen Algorithmus anzugeben, durch welchen man für jeden Werth von p eine Fundamental-Auflösung der Gleichung $\Phi = 1$ mit Leichtigkeit bestimmen könnte. Indessen, da diese Frage für die Theorie von weniger Interesse ist, und da die Methode, welche wir gefunden haben, noch viel für die Praxis zu wünschen übrig läfst, so bleibt die Lösung dieser Aufgabe für eine spätere Gelegenheit vorbehalten, und wir begnügen uns, hier die Möglichkeit und die Existenz der Fundamental-Auflösungen nachgewiesen zu haben (Vergl. §. 9. am Schlusse).

Von den associirten Formen.

§. 5.

I. Die wichtigsten Eigenschaften der Form Φ können nicht vollständig erkannt und streng bewiesen werden, ohne dafs man ein ganzes Gebiet von neuen Formen hinzunimmt und diese in Gemeinschaft mit der Form Φ betrachtet. Wenn man auf die Form Φ, deren drei lineare Factoren wir durch A, B, C bezeichnen, eine Substitution von der Form

$$(1.)\quad \begin{cases} u = \alpha\mathfrak{u} + \alpha'\mathfrak{v} + \alpha''\mathfrak{w}, \\ v = \beta\mathfrak{u} + \beta'\mathfrak{v} + \beta''\mathfrak{w}, \\ w = \gamma\mathfrak{u} + \gamma'\mathfrak{v} + \gamma''\mathfrak{w}, \end{cases} \quad \begin{Bmatrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{Bmatrix}$$

anwendet, deren Coëfficienten reelle ganze Zahlen sind und deren Determinante

$$(2.)\quad \alpha\beta'\gamma'' - \alpha\beta''\gamma' + \alpha'\beta''\gamma - \alpha'\beta\gamma'' + \alpha''\beta\gamma' - \alpha''\beta'\gamma = \Delta$$

ist, so geht die Form Φ in eine neue cubische Form mit den drei Variabeln $\mathfrak{u}$, $\mathfrak{v}$, $\mathfrak{w}$ und mit ganzen Coëfficienten über, welche, mit Ausschlufs derer von $\mathfrak{u}^3$, $\mathfrak{v}^3$, $\mathfrak{w}^3$, alle durch 3 theilbar sind. Der Linearfactor A geht durch diese Substitution in

$$(3.)\quad \{\alpha + (\beta + \gamma\varrho)\eta + (\beta + \gamma\varrho^2)\vartheta\}\mathfrak{u} + \{\alpha' + (\beta' + \gamma'\varrho)\eta - (\beta' + \gamma'\varrho^2)\vartheta\}\mathfrak{v} + \{\alpha'' + (\beta'' + \gamma''\varrho)\eta + (\beta'' + \gamma''\varrho^2)\vartheta\}\mathfrak{w} = \mathfrak{A}$$

über, während die beiden andern Linearfactoren B, C sich in die dem $\mathfrak{A}$ correspondirenden Ausdrücke verwandeln, welche wir durch $\mathfrak{B}$, $\mathfrak{C}$ bezeichnen. Setzt man der Kürze wegen

$$\begin{aligned} \alpha+(\beta+\gamma\varrho)\eta+(\beta+\gamma\varrho^2)\vartheta &= P, \\ \alpha+(\beta+\gamma\varrho)\varrho\eta+(\beta+\gamma\varrho^2)\varrho^2\vartheta &= Q, \\ \alpha+(\beta+\gamma\varrho)\varrho^2\eta+(\beta+\gamma\varrho^2)\varrho\vartheta &= R, \end{aligned}$$

PQR, welches eine reelle ganze Zahl ist, $=a$, und multiplicirt $\mathfrak{A}$ mit QR, $\mathfrak{B}$ mit PR, $\mathfrak{C}$ mit PQ, so nehmen die drei Producte $QR\mathfrak{A}$, $PR\mathfrak{B}$, $PQ\mathfrak{C}$ die Formen

$$(4.)\left\{\begin{aligned} QR\mathfrak{A} &= a\mathfrak{u}+\{b+(c+d\varrho)\eta+(c+d\varrho^2)\vartheta\}\mathfrak{v}+\{b'+(c'+d'\varrho)\eta+(c'+d'\varrho^2)\vartheta\}\mathfrak{w}, \\ PR\mathfrak{B} &= a\mathfrak{u}+\{b+(c+d\varrho)\varrho\eta+(c+d\varrho^2)\varrho^2\vartheta\}\mathfrak{v}+\{b'+(c'+d'\varrho)\varrho\eta+(c'+d'\varrho^2)\varrho^2\vartheta\}\mathfrak{w}, \\ PQ\mathfrak{C} &= a\mathfrak{u}+\{b+(c+d\varrho)\varrho^2\eta+(c+d\varrho^2)\varrho\vartheta\}\mathfrak{v}+\{b'+(c'+d'\varrho)\varrho^2\eta+(c'+d'\varrho^2)\varrho\vartheta\}\mathfrak{w} \end{aligned}\right.$$

an, so dafs die neue Form F, in welche Φ übergeht, so geschrieben werden kann:

$$(5.)\quad \frac{1}{a^2}\Big(a\mathfrak{u}+\{b+(c+d\varrho)\eta+(c+d\varrho^2)\vartheta\}\mathfrak{v}+\{b'+(c'+d'\varrho)\eta+(c'+d'\varrho^2)\vartheta\}\mathfrak{w}\Big)$$
$$(\text{etc.})\,(\text{etc.}),$$

nämlich als das Product der drei Ausdrücke zur Rechten in (4.), dividirt durch a^2. Die Buchstaben

$$(5^a.)\quad a,\ b,\ c,\ d,\ b',\ c',\ d'$$

bezeichnen reelle ganze Zahlen. Sehen wir, welche Eigenschaften diese ganzen Zahlen (5ª.) besitzen. Zuerst zeigt sich, dafs wenn man das Product der drei Factoren in den Klammern (5.) entwickelt und nach Potenzen und Producten der Variabeln $\mathfrak{u}$, $\mathfrak{v}$, $\mathfrak{w}$ ordnet, jeder Coëfficient durch a^2 theilbar sein wird: denn wenn man jeden Coëfficienten wirklich durch a^2 dividirt, so erhält man genau die Form F; welche offenbar ganze Coëfficienten hat. Wenn man die Ausdrücke für $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ als ein lineäres System von Gleichungen mit den Unbekannten $\mathfrak{u}$, $\mathfrak{v}$, $\mathfrak{w}$ ansieht ($S.$), so ist dieses System offenbar aus dem System

$$(6.)\quad \left\{\begin{aligned} A &= u+(v+w\varrho)\eta+(v+w\varrho^2)\vartheta, \\ B &= u+(v+w\varrho)\varrho\eta+(v+w\varrho^2)\varrho^2\vartheta, \\ C &= u+(v+w\varrho)\varrho^2\eta+(v+w\varrho^2)\varrho\vartheta \end{aligned}\right.$$

und aus dem System (1.) zusammengesetzt. Das System (6.) kann seinerseits wiederum als aus den beiden Systemen

$$\left.\begin{aligned} A &= u+\eta y+\vartheta z, \\ B &= u+\varrho\eta y+\varrho^2\vartheta z, \\ C &= u+\varrho^2\eta y+\varrho\vartheta z, \end{aligned}\right\}\quad \text{und}\quad \left\{\begin{aligned} u &= u, \\ y &= v+w\varrho, \\ z &= v+w\varrho^2 \end{aligned}\right.$$

zusammengesetzt betrachtet werden, d. h. aus den beiden Systemen

$$(7.)\quad \left\{\begin{matrix} 1, & \eta, & \vartheta \\ 1, & \varrho\eta, & \varrho^2\vartheta \\ 1, & \varrho^2\eta, & \varrho\vartheta \end{matrix}\right\} \quad \text{und} \quad (8.)\quad \left\{\begin{matrix} 1, & 0, & 0 \\ 0, & 1, & \varrho \\ 0, & 1, & \varrho^2 \end{matrix}\right\}.$$

Die ***Determinante*** des Systems $(S.)$ ist folglich nach einem bekannten Satze gleich dem Producte der drei Determinanten der drei Systeme (7.), (8.) und (1.). Die Determinante von (7.) ist offenbar $=\eta\vartheta(\varrho^2-\varrho+\varrho^2-\varrho+\varrho^2-\varrho)$ $=3p(\varrho^2-\varrho)$; die von (8.) ist $=\varrho^2-\varrho$, und die von (1.) ist $=\varDelta$; folglich ist die des Systems $(S.)$, $=-9p\varDelta$, mithin die Determinante des Systems (4.), $=-9a^2p\varDelta$, weil das System (4.) aus $(S.)$ entsteht, indem man die drei Horizontalreihen des letztern resp. mit QR, PR, PQ multiplicirt.

Das System (4.) kann man sich aber noch auf eine ganz andere Art entstanden vorstellen, nämlich aus Zusammensetzung von (7.), (8.) und

$$(9.)\quad \left\{\begin{matrix} a, & b, & b' \\ 0, & c, & c' \\ 0, & d, & d' \end{matrix}\right\}$$

Da die Determinante dieses letztern Systems offenbar $=a(cd'-c'd)$ ist, so erhält man für die des Systems (4.) auch

$$=-9ap(cd'-c'd).$$

Vergleicht man diesen Ausdruck mit dem vorhin für dieselbe Determinante gefundenen, so ergiebt sich

$$(10.)\quad cd'-c'd = a\varDelta.$$

Dieser Gleichung genügen also immer die in den Linearfactoren der neuen Form vorkommenden ganzen Zahlen c, c', d, d'. Ist namentlich $\varDelta=1$, so hat das umgekehrte System von (1.), welches die neuen Variabeln durch die alten ausdrückt, ebenfalls ganze Coëfficienten; denn dieses umgekehrte System wird dann

$$\left\{\begin{matrix} \beta'\gamma''-\beta''\gamma', & \alpha''\gamma'-\alpha'\gamma'', & \alpha'\beta''-\alpha''\beta' \\ \beta''\gamma'-\beta\gamma'', & \alpha\gamma''-\alpha''\gamma, & \alpha''\beta-\alpha\beta'' \\ \beta\gamma'-\beta'\gamma, & \alpha'\gamma-\alpha\gamma', & \alpha\beta'-\alpha'\beta \end{matrix}\right\},$$

durch welches man rückwärts die Form F in die Form $\varPhi$ transformiren kann. In diesem Falle nennen wir die beiden Formen $\varPhi$ und F ***aequivalent***, und man hat dann blofs

$$(11.)\quad cd'-c'd = a.$$

II. Wenn man alle in (I.) entwickelten Eigenschaften derjenigen Formen zusammenfafst, welche der Form $\varPhi$ aequivalent sind, und blofs davon

abstrahirt, dafs diese Formen aus Φ durch eine Substitution (1.) hervorgingen, gelangt man zu folgender Definition derjenigen Formen, welche wir *associirte Formen der Form* Φ nennen.

Definition.

„*Jede homogene ganze Function dritten Grades mit drei Variabeln u, v, w und reellen ganzen Coëfficienten ohne gemeinschaftlichen Theiler, welche die Form*

$$au^3+3bu^2v+3b'u^2w+3kuv^2+3k'uvw+3k''uw^2+lv^3+3l'v^2w+3l''vw^2+l'''w^3$$

hat, und welche, wenn man sie mit dem Quadrate ihres ersten Coëfficienten a^2 multiplicirt, sich als ein Product von drei correspondirenden Linearfactoren darstellen läfst, wie

$$au+\{b+(c+d\varrho)\sqrt[3]{(pp_1)}+(c+d\varrho^2)\sqrt[3]{(pp_2)}\}v+\{b'+(c'+d'\varrho)\sqrt[3]{(pp_1)}+(c'+d'\varrho^2)\sqrt[3]{(pp_2)}\}w,$$

$$au+\{b+(c+d\varrho)\varrho\sqrt[3]{(pp_1)}+(c+d\varrho^2)\varrho^2\sqrt[3]{(pp_2)}\}v+\{b'+(c'+d'\varrho)\varrho\sqrt[3]{(pp_1)}+(c'+d'\varrho^2)\varrho^2\sqrt[3]{(pp_2)}\}w,$$

$$au+\{b+(c+d\varrho)\varrho^2\sqrt[3]{(pp_1)}+(c+d\varrho^2)\varrho\sqrt[3]{(pp_2)}\}v+\{b'+(c'+d'\varrho)\varrho^2\sqrt[3]{(pp_1)}+(c'+d'\varrho^2)\varrho\sqrt[3]{(pp_2)}\}w,$$

in welchem a, b, c, d, b', c', d' reelle ganze Zahlen sind, die der Bedingung

$$(11.)\qquad cd'-c'd = a$$

genügen, heifst eine der Form Φ associirte Form."

„*Je zwei homogene Functionen dritten Grades mit 3 Variabeln und ganzen Coëfficienten heifsen aequivalent, wenn man von der einen zur andern vermittelst einer Substitution* (1.) *übergehen kann, deren Determinante Δ der Einheit $= +1$ gleich ist. Diese Beziehung ist immer eine gegenseitige.*"

Man bemerke, dafs dasjenige lineare System, welches die Linearfactoren einer associirten Form in die Variabeln der Form ausdrückt, aus den drei folgenden Systemen zusammengesetzt betrachtet werden kann:

$$\begin{Bmatrix} 1, & \eta, & \vartheta \\ 1, & \varrho\eta, & \varrho^2\vartheta \\ 1, & \varrho^2\eta, & \varrho\vartheta \end{Bmatrix}, \quad \begin{Bmatrix} 1, & 0, & 0 \\ 0, & 1, & \varrho \\ 0, & 1, & \varrho^2 \end{Bmatrix} \quad \text{und} \quad \begin{Bmatrix} a, & b, & b' \\ 0, & c, & c' \\ 0, & d, & d' \end{Bmatrix},$$

wo wir wieder der Kürze halber $\sqrt[3]{(pp_1)}=\eta$, $\sqrt[3]{(pp_2)}=\vartheta$ gesetzt haben, und wo immer $\eta\vartheta=p$ vorausgesetzt wird. Die Determinante des dritten Systems ist

$$= a(cd'-c'd) = a^2.$$

Jede der Form Φ associirte Form

$$F = au^3+3bu^2v+3b'u^2w+3kuv^2+3k'uvw+3k''uw^2+lv^3+3l'v^2w+3l''vw^2+l'''w^3$$

läfst sich auf die Form

$$F = \frac{1}{a^2}\{au+\lambda'v+\lambda''w\}\{au+\mu'v+\mu''w\}\{au+\nu'v+\nu''w\}$$

bringen, wo

$$\lambda' = b+e\eta+f\vartheta, \qquad \lambda'' = b'+e'\eta+f'\vartheta,$$
$$\mu' = b+e\varrho\eta+f\varrho^2\vartheta, \qquad \mu'' = b'+e'\varrho\eta+f'\varrho^2\vartheta,$$
$$\nu' = b+e\varrho^2\eta+f\varrho\vartheta, \qquad \nu'' = b'+e'\varrho^2\eta+f'\varrho\vartheta,$$
$$e = c+d\varrho, \quad e' = c'+d'\varrho, \quad f = c+d\varrho^2, \quad f' = c'+d'\varrho^2$$

ist, während b, c, d, b', c', d' ganze Zahlen sind und die Gleichung $cd'-c'd = a$ erfüllt ist. Entwickelt man den Ausdruck des Products für F in der zweiten Form und vergleicht diese Entwicklung mit der ersten Form, so zeigt sich, dafs die sieben folgenden Congruenzen

$$(12.)\quad \begin{cases} b^2 \equiv p\,ef \pmod{a}, \quad 2bb' \equiv p(ef'+e'f), \quad b'^2 \equiv pe'f' \pmod{a}; \\ b^3+pp_1e^3+pp_2f^3-3pbef \equiv 0 \pmod{a^2}, \\ b^2b'+pp_1e^2e'+pp_2f^2f' \equiv p(bef'+be'f+b'ef) \pmod{a^2}, \\ bb'^2+pp_1ee'^2+pp_2ff'^2 \equiv p(be'f'+b'ef'+b'e'f) \pmod{a^2}, \\ b'^3+pp_1e'^3+pp_2f'^3-3pb'e'f' \equiv 0 \pmod{a^2} \end{cases}$$

erfüllt sind.

Entwickelt man das Product der drei Factoren

$$(13.)\quad \{au+\lambda'v+\lambda''w\}\{au+\mu'v+\mu''w\}\{au+\nu'v+\nu''w\}$$

und ordnet die Entwickluug nach Potenzen und Producten der Variabeln, so ist a^2 gemeinschaftlicher Theiler aller Coëfficienten, aber zugleich ihr gröfster gemeinschaftlicher Theiler; denn sonst hätten auch die Coëfficienten der Form F einen gemeinschaftlichen Theiler; gegen die Voraussetzung.

Die sieben Congruenzen (12.), zusammen mit der Gleichung $cd'-c'd = a$, welche mit $ef'-e'f = (\varrho^2-\varrho)a$ gleichbedeutend ist, enthalten das Characteristische der associirten Formen. Letztere Gleichung läfst sich auch so aussprechen, dafs die Determinante desjenigen linearen Systems, welches sich aus den 9 Coëfficienten der drei lineären Factoren von a^2F bilden läfst, $= -9pa^2$ ist.

Wenn irgend zwei ternäre cubische Formen aequivalent sind, so ist der gröfste gemeinschaftliche Theiler der Coëfficienten der einen gleich dem gröfsten gemeinschaftlichen Theiler der Coëfficienten der andern. Denn da die beiden Formen aequivalent sind, so hat man ein lineäres System (1.), welches die erste in die zweite, und ein umgekehrtes, welches die zweite in die erste transformirt; und da von der andern Seite bei jeder Transformation die Coëfficienten der neuen Form als lineäre homogene Functionen der Coëfficienten der alten Form dargestellt werden können, folglich jeder gemeinschaftliche

Theiler, welchen diese hat, auch in jenen enthalten sein mufs, so wird nothwendig bei zwei aequivalenten Formen jeder gemeinschaftliche Theiler der Coëfficienten irgend einer von beiden auch ein gemeinschaftlicher Theiler der Coëfficienten der andern sein. Haben daher die Coëfficienten der einen von beiden *keinen* gemeinschaftlichen Theiler, so findet Dasselbe auch für die andere Statt.

Die Coëfficienten der Form Φ haben keinen gemeinschaftlichen Theiler: folglich gilt dasselbe auch für jede der Form Φ aequivalente Form. Hieraus und aus dem im Anfange dieses Paragraphen Gesagten folgt, *dafs die Form Φ sich selbst associirt und dafs jede der Form Φ aequivalente Form eine associirte Form ist;* aber es kann aufser diesen auch noch andere associirte Formen geben.

Lehrsatz 5.

„Wenn von zwei aequivalenten ternären cubischen Formen die „erste der Form Φ associirt ist, so ist auch die zweite eine asso- „ciirte Form."

Beweis. Es sei F eine associirte Form, welche durch die Substitution (1.), deren Determinante $\Delta = 1$ vorausgesetzt wird, in die Form G übergeht: es ist zu beweisen, dafs G eine associirte Form ist. Zuerst ist klar, dafs die Form G lauter ganze Coëfficienten haben wird; dafs, wie die Substitution selbst zeigt, alle diese Coëfficienten, mit Ausschlufs derer, welche in die Cuben der neuen Variabeln multiplicirt sind, durch 3 theilbar sein werden, und dafs sämmtliche Coëfficienten, wie aus dem vorhin Gesagten erhellet, keinen gemeinschaftlichen Theiler haben werden. Es bleibt nur noch zu zeigen, dafs G auf die den associirten Formen eigenthümliche Form gebracht werden kann.

Da F durch die Substitution (1.) in G übergeht, so geht a^2F, wenn a den ersten Coëfficienten von F vorstellt, durch dieselbe Substitution in a^2G über; aber a^2F ist nach der Voraussetzung gleich dem Producte dreier correspondirenden Factoren wie die in (13.): sehen wir, wie diese drei linearen Factoren sich bei der Substitution (1.) verhalten. Die drei Factoren gehen durch die erwähnte Substitution offenbar in ebenso viele neue lineäre Ausdrücke mit den neuen Variabeln der Form G über; diese letzteren Ausdrücke besitzen aber nicht mehr die Eigenschaft derer in (13.), dafs die Coëfficienten des ersten Variabeln ganze Zahlen sind, sondern in ihnen sind sämmtliche neun Coëfficienten von derselben Form, wie die Ausdrücke λ', μ', ν'. Bezeichnet man resp. durch λ, μ, ν die ersten Coëfficienten, d. h. die Coëfficienten des

ersten neuen Variabeln, in diesen drei neuen linearen Ausdrücken, so ist das Product $\lambda\mu\nu$ offenbar nichts anders, als der erste Coëfficient der Form G, welchen wir mit a_1 bezeichnen, multiplicirt mit a^2, so dafs man also $\lambda\mu\nu = a^2 a_1$ setzen kann. Multiplicirt man jetzt den ersten der drei neuen correspondirenden Ausdrücke mit $\mu\nu$, den zweiten mit $\lambda\nu$, den dritten mit $\lambda\mu$, so erhält man ein drittes System von linearen Ausdrücken; diese werden wieder dieselbe Eigenschaft haben, wie die linearen Ausdrücke in (13.), dafs die Coëfficienten der ersten Variabel ganze Zahlen sind. In der That: in allen dreien ist der Coëfficient der ersten Variabel $= a^2 a_1$, weil $\lambda\mu\nu = a^2 a_1$ ist; und überhaupt wird dieses dritte System genau von derselben Form sein, wie das in (13.). Dieses dritte System sei daher

$$(14.)\quad \begin{cases} a^2 a_1 \mathfrak{u} + \lambda_1' \mathfrak{v} + \lambda_1'' \mathfrak{w} \\ a^2 a_1 \mathfrak{u} + \mu_1' \mathfrak{v} + \mu_1'' \mathfrak{w} \\ a^2 a_1 \mathfrak{u} + \nu_1' \mathfrak{v} + \nu_1'' \mathfrak{w}, \end{cases}$$

wo gesetzt sein mag:

$$\begin{array}{ll} \lambda_1' = b_1 + e_1\eta + f_1\vartheta, & \lambda_1'' = b_1' + e_1'\eta + f_1'\vartheta, \\ \mu_1' = b_1 + e_1\varrho\eta + f_1\varrho^2\vartheta, & \mu_1'' = b_1' + e_1'\varrho\eta + f_1'\varrho^2\vartheta, \\ \nu_1' = b_1 + e_1\varrho^2\eta + f_1\varrho\vartheta, & \nu_1'' = b_1' + e_1'\varrho^2\eta + f_1'\varrho\vartheta, \end{array}$$

$$e_1 = c_1 + d_1\varrho,\quad f_1 = c_1 + d_1\varrho^2,\quad e_1' = c_1' + d_1'\varrho,\quad f_1' = c_1' + d_1'\varrho^2.$$

Das Product dieser drei Factoren in (14.) ist $= \lambda^2\mu^2\nu^2 a^2 G = a^6 a_1^2 G$, folglich hat man

$$a_1^2 G = \left\{a_1 \mathfrak{u} + \frac{\lambda_1'}{a^2}\mathfrak{v} + \frac{\lambda_1''}{a^2}\mathfrak{w}\right\}\left\{a_1 \mathfrak{u} + \frac{\mu_1'}{a^2}\mathfrak{v} + \frac{\mu_1''}{a^2}\mathfrak{w}\right\}\left\{a_1 \mathfrak{u} + \frac{\nu_1'}{a^2}\mathfrak{v} + \frac{\nu_1''}{a^2}\mathfrak{w}\right\}.$$

Es sind jetzt zwei Behauptungen zu beweisen: erstlich, dafs

$$\frac{b_1}{a^2},\ \frac{c_1}{a^2},\ \frac{d_1}{a^2},\ \frac{b_1'}{a^2},\ \frac{c_1'}{a^2},\ \frac{d_1'}{a^2}$$

ganze Zahlen sind, und zweitens, dafs

$$\frac{c_1}{a^2}.\frac{d_1'}{a^2} - \frac{c_1'}{a^2}.\frac{d_1}{a^2} = a_1$$

ist. Man sieht, dafs, sobald diese beiden Behauptungen bewiesen sein werden, die Richtigkeit des Satzes aufser Zweifel gestellt sein wird. Wir beginnen mit dem Beweise der zweiten Behauptung.

Dieselbe verlangt nichts anders zu beweisen, als dafs die Determinante des linearen Systems

$$\left\{\begin{matrix} a_1, & \frac{\lambda'_1}{a^2}, & \frac{\lambda''_1}{a^2} \\ a_1, & \frac{\mu'_1}{a^2}, & \frac{\mu''_1}{a^2} \\ a, & \frac{\nu'_1}{a^2}, & \frac{\nu''_1}{a^2} \end{matrix}\right\} = (S.),$$

$= -9pa_1^2$ ist. Diese Determinante des Systems $(S.)$, deren Werth wir suchen und welche für den Augenblick durch D bezeichnet werden mag, ist offenbar $= \frac{1}{a^6}$ mal die Determinante desjenigen Systems, welches aus den 9 Coëfficienten der drei correspondirenden Ausdrücke (14.) gebildet werden kann. Diese letztere Determinante ist ihrerseits gleich $\lambda^2\mu^2\nu^2$ mal die Determinante desjenigen Systems, in welches die drei correspondirenden Factoren von a^2F durch die Substitution (1.) übergehen: eines Systems, welches folglich aus den beiden Systemen

$$\left\{\begin{matrix} a, & \lambda', & \lambda'' \\ a, & \mu', & \mu'' \\ a, & \nu', & \nu'' \end{matrix}\right\} = (T.)$$

und (1.) zusammengesetzt ist. Da nun die Determinante von (1.) $= 1$ und die von $(T.)$ nach der Voraussetzung $= -9pa^2$ ist, so erhält man $D = \frac{1}{a^6}.\lambda^2\mu^2\nu^2.(-9pa^2)$. Aber $\lambda^2\mu^2\nu^2 = a^4a_1^2$, folglich $D = -9pa_1^2$; was zu beweisen war.

Um die erste Behauptung zu beweisen, entwickle ich das Product der drei Factoren (14.), von welchem Product, da es $= a^6a_1^2G$ ist, nach Potenzen und Producten der Variabeln $\mathfrak{u}, \mathfrak{v}, \mathfrak{w}$ geordnet, alle Coëfficienten, selbst abgesehen von den numerischen Multiplicatoren 3, durch $a^6a_1^2$ theilbar sein werden. Betrachtet man in der Entwicklung dieses Products namentlich die Coëfficienten von $\mathfrak{u}^2\mathfrak{v}$, $\mathfrak{u}\mathfrak{v}^2$ und $\mathfrak{v}^3$, so zeigt sich, dafs die folgenden drei Congruenzen:

$$b_1 \equiv 0 \pmod{a^2}, \qquad b_1^2 \equiv pe_1f_1 \pmod{a^4},$$
$$b_1^3 + pp_1e_1^3 + pp_2f_1^3 - 3pb_1e_1f_1 \equiv 0 \pmod{a^6}$$

Statt finden, von denen die erste schon zeigt, dafs b_1 durch a^2 theilbar ist. Vermöge der ersten und zweiten nimmt die dritte Congruenz die einfachere Gestalt

$$(15.)\qquad pp_1e_1^3 + pp_2f_1^3 \equiv 0 \pmod{a^6} \text{ an.}$$

Ich behaupte, dafs die complexen Zahlen e_1 und f_1 beide durch a^2 theilbar sind. In der That: es sei ω irgend ein *complexer* Primfactor von a^2, und ω^n die höchste in a^2 aufgehende Potenz von ω. Wäre nun z. B.

e_1 nicht durch ω^n, sondern nur durch eine niedrigere Potenz von ω theilbar, so müfste der Exponent der höchsten in e_1^3 aufgehenden Potenz von ω wenigstens um 3 Einheiten kleiner sein als $3n$, also müfste für $pp_1e_1^3$ dieser Exponent wenigstens um eine Einheit kleiner sein als $3n$, folglich müfste wegen der Congruenz (15.), welche auch nach dem Modul ω^{3n} Statt findet, auch der höchste Exponent von ω für $pp_2f_1^3$ wenigstens um 1 kleiner sein als $3n$; und um so mehr gilt dies also von f_1^3 *). Da also der höchste Exponent von ω in e_1 sowohl als in f_1 kleiner als n wäre, so müfste er im Producte e_1f_1 wenigstens um 2, also in pe_1f_1 wenigstens um eine Einheit unter $2n$ liegen **). Dies letztere widerstreitet aber der Congruenz $pe_1f_1 \equiv 0$ (mod. a^4), welche aus den beiden ersten der oben aufgestellten Congruenzen folgt. Mithin ist die obige Annahme falsch, und es ist in der That e_1 durch ω^n theilbar; folglich ist, da dieses Raisonnement für jeden complexen Primfactor von a^2 gilt, auch e_1 durch a^2 theilbar. Aber $e_1 = c_1 + d_1\varrho$, und a^2 ist reell, folglich sind auch c_1 und d_1 durch a^2 theilbar. Untersucht man statt der Coëfficienten von $\mathfrak{u}^2\mathfrak{v}$, $\mathfrak{u}\mathfrak{v}^2$, $\mathfrak{v}^3$ die von $\mathfrak{u}^2\mathfrak{w}$, $\mathfrak{u}\mathfrak{w}^2$, $\mathfrak{w}^3$, und wendet wörtlich dieselben Schlufsfolgen an, mit dem einzigen Unterschiede, dafs man die Buchstaben b_1, e_1, f_1 accentuirt, so zeigt sich, dafs b_1', c_1', d_1' durch a^2 theilbar sind. Der Satz ist also vollständig bewiesen.

Wir bemerken, dafs Alles, was der Lehrsatz behauptet, auch durch Rechnung, d. h. durch wirkliche Substitution von (1.) abgeleitet werden kann. Da jedoch diese Rechnung sehr mühsam und weitläufig ist, und jedes durch Rechnung gewonnene Resultat mehr oder weniger den Schein des Zufälligen an sich trägt, so glaubten wir besser zu thun, wenn wir den Beweis des Satzes blofs auf eine Reihe von Schlüssen gründeten.

An den eben bewiesenen Fundamentalsatz, durch welchen erst eine Behandlung der associirten Formen möglich wird, schliefsen sich folgende Betrachtungen an.

Wenn sich unter einer Reihe von beliebig vielen *aequivalenten* ternären cubischen Formen eine einzige *associirte* Form befindet, so sind sie alle associirte Formen; und umgekehrt, wenn irgend eine derselben der Form Φ *nicht associirt* ist, so kann es auch keine derselben sein.

---

*) Da $pp_1 = p_1^2p_2$ ist, so kann dieser Factor höchstens das Quadrat von ω hinzubringen, nämlich ω^2, wenn $\omega = p_1$, ω, wenn $\omega = p_2$ und gar kein neues ω, wenn ω von p_1 sowohl als von p_2 verschieden ist.

**) Der Factor $p = p_1p_2$ bringt ein einziges neues ω hinzu, wenn $\omega = p_1$ oder $= p_2$; in andern Fällen bringt dieser Factor gar kein neues ω hinzu.

Wenn eine associirte Form einer zweiten und diese einer dritten aequivalent ist, so ist auch die erste der dritten aequivalent. Es gehe die Form F durch eine Substitution S, deren Determinante $= 1$ ist, in die Form G über, und es gehe G durch eine Substitution T, deren Determinante ebenfalls $= 1$ ist, in die Form H über: sodann geht offenbar F in H über, durch die aus S und T zusammengesetzte Substitution, welche wir durch $S \times T$ bezeichnen; die Coëfficienten dieser neuen Substitution sind nothwendig ganze Zahlen, weil die von S und T als solche vorausgesetzt werden, und ihre Determinante ist gleich dem Producte der Determinanten der beiden Substitutionen S und T, also $= 1$; folglich sind die beiden Formen F und H in der That aequivalent.

Wenn in einer Reihe von beliebig vielen associirten Formen jede ihrer folgenden aequivalent ist, so ist auch die erste der letzten und jede beliebige Form dieser Reihe jeder beliebigen andern derselben Reihe aequivalent.

Alle der Form Φ associirten Formen können folglich in *Classen* eingetheilt werden, wenn man je zwei associirte Formen in dieselbe oder in verschiedene Classen aufnimmt, je nachdem sie aequivalent sind, oder nicht. Die Form Φ selbst, mit allen ihren aequivalenten Formen, bildet die erste Classe. Sind nun noch aufserdem associirte Formen vorhanden, so nehme man irgend eine von ihnen; sie bildet mit allen ihr aequivalenten Formen die zweite Classe. Von den dann noch vorhandenen nehme man wiederum irgend eine und vereinige sie mit allen ihr aequivalenten in die dritte Classe, und so weiter fort, bis alle associirten Formen erschöpft sind. Wenn man, nachdem diese Classification ausgeführt ist, aus jeder Classe *eine* Form nach Belieben herausnimmt, so wird ein solches System offenbar die doppelte Eigenschaft haben, dafs jede associirte Form einer, aber auch nur einer von ihnen aequivalent ist.

III. Wenn man aus einer associirten Form F zwei andere bildet, indem man von den drei linearen Factoren, in welche sich $a^2 F$ zerlegen läfst, den *zweiten* zum *ersten* (also auch den dritten zum zweiten, den ersten zum dritten), oder den *dritten* zum *ersten* (also auch den ersten zum zweiten, den zweiten zum dritten) macht, so heifsen, F mitgerechnet, diese drei Formen *correspondirende Formen;* das Schema für correspondirende Formen ist, wenn man die drei linearen Formen von $a^2 F$ durch 1, 2, 3 bezeichnet,

1,	2,	3
2,	3,	1
3,	1,	2

Obgleich correspondirende Formen in Beziehung auf ihre Coëfficienten vollkommen mit einander übereinstimmen, so werden sie doch in der gegenwärtigen Theorie als *verschiedene* Formen angesehen. Damit zwei associirte Formen als *identisch* betrachtet werden können, ist nöthig, dafs man sich die Producte aus den Formen in die Quadrate ihrer ersten Coëfficienten auf die Weise in Factoren zerlegt vorstellt, dafs der erste Factor mit dem ersten Factor, der zweite mit dem zweiten, der dritte mit dem dritten übereinstimmt. In demselben Sinne ist Alles zu nehmen, was später über Transformation der associirten Formen gesagt werden wird. Wenn wir z. B. von Transformationen sprechen, welche eine associirte Form F in sich selbst übergehen lassen, so meinen wir immer solche, welche, abgesehen von constanten Multiplicatoren, jeden der drei lineären Factoren in sich selbst verwandeln, während die übrigen Substitutionen (wenn es deren geben sollte), welche eine Vertauschung der Linearfactoren bewirken, nicht sowohl als Transformationen von F in sich selbst, sondern vielmehr als Transformationen von F in eine ihrer correspondirenden Formen betrachtet werden. Eben so: wenn die associirte Form F in die Form G durch die Substitution S übergeht und wir suchen alle Substitutionen, welche dieselbe Wirkung hervorbringen, so meinen wir nur solche, welche den zu G gehörigen Linearfactoren *dieselbe* Ordnung bewahren, die sie durch die Substitution S erhalten haben, während die übrigen vielmehr als Substitutionen von F in eine der G correspondirende Form angesehen werden. Die Wichtigkeit dieser Unterscheidung zeigt sich besonders bei der Classification der associirten Formen, und ihre Vernachlässigung kann zu grofsen Verwirrungen Anlafs geben. Bei den quadratischen Formen ist eine solche Unterscheidung überflüssig, weil *nie* eine quadratische Form sich selbst in dem Sinne (eigentlich) aequivalent sein kann, dafs ihre Linearfactoren bei der Substitution eine Vertauschung erlitten (vergleichen *Dirichlet*, „Sur les formes quadratiques. §. 11. Remarque." im 24ten Bande dieses Journals), so dafs je zwei Formen, welche durch Permutation der beiden Linearfactoren aus einander entstehen, immer in verschiedene Classen gehören würden und dafs man also auf nichts anders hinauskäme, als jede Classe doppelt zu schreiben; was gar keinen Vortheil gewähren würde. Ganz anders verhält es sich hier bei den cubischen Formen; für gewisse associirte Formen können die drei correspondirenden Formen aequivalent sein, während dies für andere associirte Formen nicht der Fall ist; in gewisser Fällen können also drei correspondirende Formen in dieselbe Classe gehören, während sie in andern Fällen in drei verschiedene

Classen gerechnet werden müssen. Die Form Φ z. B. befindet sich immer in dem ersten Falle, denn sie geht in ihre correspondirenden Formen durch die Substitutionen resp.

$$\begin{Bmatrix} 1, & 0, & 0 \\ 0, & 0, & -1 \\ 0, & 1, & -1 \end{Bmatrix}, \quad \begin{Bmatrix} 1, & 0, & 0 \\ 0, & -1, & 1 \\ 0, & -1, & 0 \end{Bmatrix}$$

über, welche beide die Determinante $=+1$ haben. Wir verbreiten uns über diesen Gegenstand ausführlich, weil er eine Unterscheidung betrifft, die in den frühern Gebieten der Zahlentheorie kein Analogon findet und welche für die gesammte Theorie der höhern Formen von Wichtigkeit ist. Sie ist einfach genug; aber die Unterlassung derselben mufs, wie schon bemerkt, zu Verwirrungen führen, indem sie Classen von Formen zusammenfallen läfst, die ihrer Natur nach getrennt dastehen.

Der Einfachheit wegen bleiben von unserer Untersuchung alle diejenigen associirten Formen als *uneigentliche Formen* ausgeschlossen, in welchen die Coëfficienten von u^3, v^3, w^3, uvw sämmtlich gerade und wo zugleich in jeder der drei binären cubischen Formen, welche man erhält, wenn man nach und nach $u=0$, $v=0$, $w=0$ setzt, die beiden mittleren Coëfficienten entweder beide zugleich gerade, oder beide zugleich ungerade sind; solche uneigentliche Formen können für alle möglichen Werthe der Variabeln nur ausschliefslich *geraden* Zahlen gleich werden, während die übrigen Formen, welche wir als *eigentlich* bezeichnen, sowohl geraden als ungeraden Zahlen gleich werden können. Es folgt hieraus, dafs jede einer uneigentlichen Form aequivalente Form ebenfalls eine uneigentliche Form sein mufs; alle uneigentlichen Formen sind also in gewissen Classen enthalten, während die übrigen Classen, zu denen immer die Classe der Grundform Φ (die Fundamentalclasse) gehört, die eigentlichen Formen enthalten. Wir betrachten nur die eigentlichen Formen; und wenn wir in der Folge blofs von associirten Formen reden, so meinen wir solche, in denen *nicht* zugleich die Bedingungen erfüllt sind, dafs die Coëfficienten von u^3, v^3, w^3, uvw sämmtlich gerade und in jeder der oben bezeichneten binären Formen die mittleren Coëfficienten beide gerade oder beide ungerade sind. Wir empfehlen übrigens Dem, welcher diese Untersuchungen üben will, die Behandlung der uneigentlichen associirten Formen.

Von der Darstellung der Zahlen durch associirte Formen.

§. 6.

Nachdem in dem vorigen Paragraph die einfachsten Eigenschaften der associirten Formen behandelt worden sind, gehen wir zu der Theorie der Darstellung von ganzen Zahlen durch associirte Formen über.

Eine reelle ganze Zahl M heifst durch eine associirte Form F *darstellbar,* wenn man ihren Variabeln solche reelle ganze Werthe $u=\alpha$, $v=\beta$, $w=\gamma$ geben kann, dafs für dieselben der Werth der Form $=M$ wird. Die Darstellung heifst eine *eigentliche,* wenn die Werthe der Variabeln α, β, γ keinen gemeinschaftlichen Theiler haben; im entgegengesetzten Falle eine *uneigentliche.* Wenn M durch F darstellbar ist, so ist auch $-M$ durch F darstellbar, und auf eben so viele Arten; denn man braucht den Variabeln nur entgegengesetzte Werthe $-\alpha$, $-\beta$, $-\gamma$ zu geben. Wir betrachten zuerst die eigentlichen, später die uneigentlichen Darstellungen.

I. *Hülfssatz.* „Wenn α, β, γ drei gegebene ganze Zahlen ohne gemeinschaftlichen Theiler sind, so kann man immer auf unendlich viele Arten 6 ganze Zahlen α', β', γ', α'', β'', γ'' finden, von der Art, dafs die Determinante des lineären Systems

$$(1.)\quad \begin{Bmatrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{Bmatrix} = S$$

der positiven Einheit gleich wird."

Wir bezeichnen das eben geschriebene lineäre System durch S, seine Determinante

$$\alpha(\beta'\gamma''-\beta''\gamma')+\beta(\alpha''\gamma'-\alpha'\gamma'')+\gamma(\alpha'\beta''-\alpha''\beta')$$

durch Δ; dann sind α' etc. so zu bestimmen, dafs $\Delta=1$ wird. Nach *Gaufs* „Disquisitiones arithm. No. 40." kann man, da α, β, γ keinen gemeinschaftlichen Theiler haben, drei ganze Zahlen A, B, C so bestimmen, dafs $\alpha A+\beta B+\gamma C=1$ wird, und nach Disq. arithm. No. 279. kann man ganze Werthe für α', β' etc. finden, welche den Gleichungen $\beta'\gamma''-\beta''\gamma'=A$, $\alpha''\gamma'-\alpha'\gamma''=B$, $\alpha'\beta''-\alpha''\beta'=C$ genügen: folglich kann man in der That ganze Werthe von α', β' etc. bestimmen, welche $\Delta=1$ machen. Alles kommt also nur darauf an, aus *einer* Lösung des Problems alle möglichen abzuleiten. Setzen wir zu dem Ende ein bestimmtes der Systeme S, in denen die ersten Coëfficienten der drei Horizontalreihen resp. α, β, γ sind, mit

dem Systeme

$$\begin{Bmatrix} I, & K, & L \\ I', & K', & L' \\ I'', & K'', & L'' \end{Bmatrix} = T$$

zusammen, und sehen welche Bedingung die Coëfficienten des Systems T erfüllen müssen, damit das aus der Zusammensetzung entstehende System ebenfalls resp. α, β, γ zu ersten Coëfficienten seiner drei Horizontalreihen hat. Diese Bedingung ist ausgesprochen durch die folgenden drei Gleichungen:

$$\alpha I + \alpha' I' + \alpha'' I'' = \alpha, \quad \beta I + \beta' I' + \beta'' I'' = \beta, \quad \gamma I + \gamma' I' + \gamma'' I'' = \gamma,$$

welche für I, I', I'' die vollkommen bestimmten Werthe $I = 1$, $I' = 0$, $I'' = 0$ liefern. Damit aber die Determinante des zusammengesetzten Systems ebenfalls $= 1$ wird, ist nöthig, dafs die Determinante des Systems T, nämlich die des Systems

$$(2.) \quad \begin{Bmatrix} 1, & K, & L \\ 0, & K', & L' \\ 0, & K'', & L'' \end{Bmatrix} = T,$$

$= 1$, also dafs $K'L'' - K''L' = 1$ ist. Wenn man daher nach und nach statt K und L alle möglichen ganzen Zahlen und statt K', L', K'', L'' alle ganzen Zahlen setzt, welche der Bedingung

$$(3.) \quad K'L'' - K''L' = 1$$

genügen, und mit allen diesen unendlich vielen Systemen T das ursprüngliche System S zusammensetzt, so erhält man lauter neue Systeme, welche alle der Bedingung genügen, dafs ihre drei ersten Coëfficienten α, β, γ sind und dafs ihre Determinante $= 1$ ist. Umgekehrt behaupte ich, dafs man auf diese Weise alle Systeme erhält, welche den beiden eben erwähnten Bedingungen genügen; und keines derselben doppelt. Um diese Behauptung zu erweisen, ist nur nöthig, zu zeigen, dafs man, wenn S' irgend ein zweites von S verschiedenes System bezeichnet, dessen erste Coëfficienten (und wir verstehen darunter immer die drei Coëfficienten der ersten Verticalreihe) α, β, γ sind, und dessen Determinante $= 1$ ist, immer ein System von der Form T (2.) und nur ein einziges aufstellen kann, welches mit S zusammengesetzt das System S' hervorbringt. Bildet man das umgekehrte System des Systems S, welches nicht unpassend durch $\frac{1}{S}$ bezeichnet werden kann, so wird dieses System ganze Coëfficienten und die Einheit zur Determinante haben, weil die Determinante von S der Einheit gleich ist; dieses letztere System mit S' zusammengesetzt giebt ein drittes System, ebenfalls mit ganzen Coëfficienten und

der Determinante $=1$, welches durch $\frac{1}{S}\times S'$ bezeichnet sein wird. Das System S, mit diesem dritten Systeme zusammengesetzt, bringt das System S' hervor. In der That ist

$$S\times\left(\frac{1}{S}\times S'\right)=S\times\frac{1}{S}\times S'=\begin{Bmatrix}1,0,0\\0,1,0\\0,0,1\end{Bmatrix}\times S'=S'.$$

Aber es giebt auch nur dies einzige System, mit welchem S zusammengesetzt S' hervorbringt; denn es sei X irgend ein noch unbekanntes System, welches der Bedingung $S\times X=S'$ genügt: setzt man $\frac{1}{S}$ mit beiden Seiten dieser Gleichung zusammen und bemerkt, dafs $\frac{1}{S}\times S\times X=X$ ist, so erhält man $X=\frac{1}{S}\times S'$. Es bleibt also nur noch zu zeigen, dafs das System $\frac{1}{S}\times S'$ in der Form (2.) enthalten ist. Es sei dieses System $\frac{1}{S}\times S'=\begin{Bmatrix}I, & K, & L\\I', & K', & L'\\I'', & K'', & L''\end{Bmatrix}$; da S mit dem eben geschriebenen Systeme zusammengesetzt S' hervorbringt, also ein System, dessen erste Coëfficienten α, β, γ sind, so folgt, wie oben, $I=1$, $I'=0$, $I''=0$; und da die Determinante des Systems $\frac{1}{S}\times S'$ der Einheit gleich ist, so hat man nothwendig $K'L''-K''L'=1$. Unsere Behauptung ist also jetzt vollständig erwiesen.

Da das System (2.) seinerseits in die beiden Systeme

$$\begin{Bmatrix}1, & 0, & 0\\0, & K', & L'\\0, & K'', & L''\end{Bmatrix}\times\begin{Bmatrix}1, & K, & L\\0, & 1, & 0\\0, & 0, & 1\end{Bmatrix}$$

zerlegt werden kann, so können wir das Resultat der Untersuchung in folgendem Satze aussprechen:

„Es giebt immer unendlich viele lineäre Systeme dritter Ordnung, d. h mit drei Variabeln und ganzen Coëfficienten, deren drei erste Coëfficienten α, β, γ sind und deren Determinante $=1$ ist; und bezeichnet man durch S irgend eines derselben, so erhält man sie alle nach der Reihe, wenn man das System S mit den beiden Systemen

$$(4.)\quad\begin{Bmatrix}1, & 0, & 0\\0, & \varphi, & \chi\\0, & \psi, & \omega\end{Bmatrix}\times\begin{Bmatrix}1, & m, & n\\0, & 1, & 0\\0, & 0, & 1\end{Bmatrix}$$

zusammensetzt, in welchen φ, χ, ψ, ω alle ganzen Zahlen, die der

Gleichung $\varphi\omega-\chi\psi=1$ genügen, und m, n alle möglichen ganzen Zahlen vorstellen."

II. *Aufgabe.* „Wenn a eine gegebene ganze Zahl ist: alle ganzen Zahlen c, c', d, d' zu finden, welche der Bedingung $cd'-c'd=a$ genügen."

Die Aufgabe kommt darauf hinaus, alle linearen Systeme zweiter Ordnung $\begin{Bmatrix} c, & c' \\ d, & d' \end{Bmatrix}$ zu finden, deren Coëfficienten ganz sind und deren Determinante $=a$ ist. Es ist leicht, die Existenz solcher Systeme einzusehen; denn man braucht nur c, c' ganz beliebig anzunehmen, doch so, dafs ihr gröfster gemeinschaftlicher Theiler in a aufgeht, und kann dann immer d, d' auf unendlich viele Arten dazu bestimmen. Wenn man eines dieser Systeme $\begin{Bmatrix} c, & c' \\ d, & d' \end{Bmatrix}$ mit allen möglichen Systemen $\begin{Bmatrix} \varphi, & \chi \\ \psi, & \omega \end{Bmatrix}$ zusammensetzt, deren Determinante $\varphi\omega-\chi\psi=1$ ist, so erhält man unendlich viele Systeme, deren Determinante $=a$ ist; alle auf diese Weise entstehenden Systeme $\begin{Bmatrix} C, & C' \\ D, & D' \end{Bmatrix}$ bezeichnen wir als eine *Gruppe* von Systemen. Alle Systeme einer Gruppe sind folglich in den Formeln

$$C=c\varphi+c'\psi, \quad C'=c\chi+c'\omega,$$
$$D=d\varphi+d'\psi, \quad D'=d\chi+d'\omega$$

enthalten. Es sei t der gröfste gemeinschaftliche Theiler der beiden Zahlen c und c', so dafs, wegen der Gleichung $cd'-c'd=a$, t ein Factor von a sein wird; es sei $a=tt'$. Da $\frac{c}{t}$, $\frac{c'}{t}$ relative Primzahlen sind, so hat die Gleichung $\frac{c}{t}\varphi+\frac{c'}{t}\psi=1$, d. h. die Gleichung $C=t$, unendlich viele Auflösungen φ und ψ; wird eine dieser Auflösungen durch φ_0, ψ_0 bezeichnet, so ist die allgemeine Auflösung der Gleichung $C=t$:

$$\varphi=\varphi_0-k\frac{c'}{t}, \quad \psi=\psi_0+k\frac{c}{t}.$$

Soll nun noch $C'=0$ sein, so mufs man, damit die Gleichung $\varphi\omega-\chi\psi=1$ erfüllt werde, nothwendig $\chi=-\frac{c'}{t}$, $\omega=\frac{c}{t}$ setzen. Die eben geschriebenen Werthe von φ und ψ, in den Ausdruck für D gesetzt, geben

$$D=d\varphi_0+d'\psi_0+k\frac{cd'-c'd}{t}=d\varphi_0+d'\psi_0+kt';$$

woraus man sieht, dafs immer ein, aber auch nur ein Werth von k, also immer ein, aber auch nur ein System φ, ψ existirt, für welches D der Bedingung

$$0 \leqq D < t'$$

genügt. Die Werthe von χ und ω in den Ausdruck für D' gesetzt, geben

$$D' = \frac{cd'-c'd}{t} = \frac{a}{t} = t'.$$

Hieraus ergiebt sich, dafs immer ein System, aber nur ein System $\begin{Bmatrix} \varphi, & \chi \\ \psi, & \omega \end{Bmatrix}$ existirt, mit welchem $\begin{Bmatrix} c, & c' \\ d, & d' \end{Bmatrix}$ zusammengesetzt ein System von der Form

$$(5.) \quad \begin{Bmatrix} t, & 0 \\ \xi, & t' \end{Bmatrix}$$

hervorbringt, in welchem t der gröfste gemeinschaftliche Theiler von c und c', $t' = \frac{a}{t}$ und ξ eine ganze Zahl aus der Reihe

$$0, 1, 2, 3, \ldots\ldots t'-1$$

ist. Jede Gruppe enthält also ein System von dieser Form (5.), welches dazu dienen kann, die ganze Gruppe zu characterisiren; und bedenkt man, dafs irgend ein System von der Form $\begin{Bmatrix} \varphi, & \chi \\ \psi, & \omega \end{Bmatrix}$, mit allen Systemen dieser Form zusammengesetzt, wiederum alle Systeme dieser Form hervorbringt, so sieht man, dafs die Formel

$$(6.) \quad \begin{Bmatrix} t, & 0 \\ \xi, & t' \end{Bmatrix} \times \begin{Bmatrix} \varphi, & \chi \\ \psi, & \omega \end{Bmatrix}$$

alle Systeme derjenigen Gruppe ausdrückt, in welcher das System (5.) enthalten ist.

Von der andern Seite sieht man, dafs alle Systeme, welche (5.) enthält, wenn man nach und nach statt t alle Factoren der Zahl a, $t' = \frac{t}{a}$, und zu jedem Werthe von t nach und nach für ξ alle Glieder der Reihe 0, 1, 2, 3, ... $t'-1$ einführt, der Bedingung genügen, dafs ihre Determinante $= a$ wird; denn diese Determinante ist $= tt' - 0.\xi = a$. Jedem dieser Systeme (5.) entspricht also wirklich eine Gruppe von Systemen; so dafs die Anzahl der Gruppen von Systemen, deren Determinante $= a$ ist, gleich ist der Anzahl der Systeme (5.), und dafs man alle Gruppen von Systemen erhält, wenn man in die Formel (6.) statt t alle Factoren von a und zu jedem Factor für ξ alle Zahlen der Reihe 0, 1, 2, 3, ... $t'-1$ einführt. Es folgt hieraus, dafs die Anzahl der Gruppen gleich ist der *Summe der Factoren* der Zahl a; nämlich $= \Sigma t'$. Die in (5.) enthaltenen $\Sigma t'$ Systeme heifsen *reducirte Systeme mit der Determinante* a.

Nach diesen vorbereitenden Untersuchungen kommen wir zur Darstellung der Zahlen.

III. Es sei a eine reelle positive ganze Zahl, welche durch die associirte Form G darstellbar ist, wenn man den Variabeln die Werthe resp. α, β, γ giebt, welche ohne gemeinschaftlichen Theiler vorausgesetzt werden. Wählt man 6 ganze Zahlen α', β', γ', α'', β'', γ'', welche der Bedingung genügen, dafs die Determinante des Systems (1.) $= 1$ wird, und wendet auf die Form G die Substitution (1.) an, so erhält man eine neue, der G aequivalente Form F; *der erste Coëfficient dieser neuen Form wird* $= a$ *sein;* denn dieser erste Coëfficient ist nichts anders als der Werth der Form G, wenn man statt der Variabeln resp. α, β, γ substituirt. Da man nach dem Obigen α', β' etc. auf unendlich viele Arten bestimmen kann, so wollen wir sehen, welche Beziehung alle die unendlich vielen neuen Formen unter einander haben, in welche G durch Anwendung aller der Substitutionen übergeht, deren erste Verticalreihe $\begin{matrix}\alpha\\ \beta\\ \gamma\end{matrix}$ und deren Determinante $= 1$ ist. Da alle Substitutionen dieser Art aus irgend einer von ihnen gefunden werden, wenn man diese letztere mit allen möglichen in der Formel (4.) enthaltenen Substitutionen zusammensetzt, so werden auch alle neuen Formen, deren Inbegriff wir durch ($\mathfrak{F}$) bezeichnen, aus einer derselben F hervorgehen, wenn man auf diese nach der Reihe alle Substitutionen (4.) anwendet. Da die Substitution (4.) eine zusammengesetzte ist, so wollen wir die beiden Substitutionen, in welche sie zerlegt werden kann, nach einander anwenden; also erst die Substitution

$$(7.)\qquad v = \varphi v_1 + \chi w_1, \qquad w = \psi v_1 + \omega w_1,$$

in welcher $\varphi\omega - \chi\psi = 1$ ist, und dann die Substitution

$$(8.)\qquad u = u_1 + m v_1 + n w_1,$$

in welcher m und n alle möglichen ganzen Zahlen vorstellen. Es sei, da F eine associirte Form ist und den ersten Coëfficienten a hat:

$$a^2 F = (au + \lambda v + \lambda' w)(au + \mu v + \mu' w)(au + \nu v + \nu' w),$$

$$\lambda = b + (c + d\varrho)\eta + (c + d\varrho^2)\vartheta, \qquad \lambda' = b' + (c' + d'\varrho)\eta + (c' + d'\varrho^2)\vartheta,$$

$$\mu = b + (c + d\varrho)\varrho\eta + (c + d\varrho^2)\varrho^2\vartheta, \qquad \mu' = b' + (c' + d'\varrho)\varrho\eta + (c' + d'\varrho^2)\varrho^2\vartheta,$$

$$\nu = b + (c + d\varrho)\varrho^2\eta + (c + d\varrho^2)\varrho\vartheta, \qquad \nu' = b' + (c' + d'\varrho)\varrho^2\eta + (c' + d'\varrho^2)\varrho\vartheta,$$

wo b, c, d, b', c', d' ganze Zahlen sind und $cd' - c'd = a$ ist. Es gehe F durch die Substitution (7.) in F_1, und F_1 durch die Substitution (8.) in die associirte Form F_2 über: dann werden $a^2 F$, $a^2 F_2$ genau dieselbe Form

haben, wie $a^2 F$, indem nur andere ganze Werthe an die Stelle von b, c, d, b', c', d' treten. In Beziehung auf $a^2 F_1$ gehen diese ganzen Zahlen b, c, etc. resp. in

$$b_1 = b\varphi + b'\psi, \quad c_1 = c\varphi + c'\psi, \quad d_1 = d\varphi + d'\psi,$$
$$b_1' = b\chi + b'\omega, \quad c_1' = c\chi + c'\omega, \quad d_1' = d\chi + d'\omega$$

über. Betrachtet man die Werthe von c_1, c_1', d_1, d_1' näher, so sieht man, dafs das System $\begin{Bmatrix} c_1, & c_1' \\ d_1, & d_1' \end{Bmatrix}$ als zusammengesetzt aus den beiden Systemen

$$\begin{Bmatrix} c, & c' \\ d, & d' \end{Bmatrix} \times \begin{Bmatrix} \varphi, & \chi \\ \psi, & \omega \end{Bmatrix}$$

betrachtet werden kann; und da $cd' - c'd = a$ ist, so erhellet aus dem oben über die Gruppen von Systemen mit der Determinante a Gesagten, dafs sich unter allen den Substitutionen (7.) eine, aber auch nur eine befindet, für welche

$$(\mathfrak{A}.) \qquad c_1 = t, \quad c_1' = 0, \quad d_1 = \xi, \quad d_1' = t'$$

ist, wo $tt' = a$ und ξ eine Zahl aus der Reihe 0, 1, 2, 3, ... $t'-1$ ist. Wählen wir unter allen Substitutionen (7.) gerade diese bestimmte aus und wenden sie auf die Form F an, so haben in der Form F_1 die Zahlen c_1, c_1', d_1, d_1' genau die eben geschriebenen Werthe.

Die Substitution (8.), zu welcher wir jetzt übergehen, auf die Form F_1 angewandt, welche sie in F_2 transformirt, läfst offenbar c_1, c_1', d_1 und d_1' unverändert, so dafs

$$c_2 = c_1 = t, \quad c_2' = c_1' = 0, \quad d_2 = d_1 = \xi, \quad d_2' = d_1' = t'$$

ist, während b_1, b_1' resp. in

$$(\mathfrak{B}.) \qquad b_2 = b_1 + ma, \quad b_2' = b_1' + na$$

übergehen. In diesen letztern Formeln giebt es einen Werth von m, und nur einen, für welchen $0 \leqq b_2 < a$, und ebenso einen, und nur einen Werth von n, für welchen $0 \leqq b_2' < a$ ist: folglich giebt es eine, und nur eine Substitution unter den unendlich vielen (8.), welche F_1 in eine Form übergehen läfst, in der die beiden eben geschriebenen Bedingungen erfüllt sind.

Aus dieser Discussion folgt, dafs unter der Gesammtheit der Formen ($\mathfrak{F}$.) *immer eine*, und *nur eine* gefunden werden kann, für welche man gleichzeitig

$$(9.) \quad 0 \leqq b < a, \quad c = t, \quad 0 \leqq d < t', \quad 0 \leqq b' < a, \quad c' = 0, \quad d' = t'$$

hat. Jede associirte Form, deren erster Coëfficient a ist, und für welche die eben geschriebenen 6 Bedingungen erfüllt sind, während tt' irgend eine Zerlegung der Zahl a in das Product zweier (reellen) Factoren vorstellt, heifst

eine ***reducirte Form mit dem ersten Coëfficienten a,*** oder eine ***zu a gehörige reducirte Form.***

Unter der Gesammtheit der Formen (𝔍.) befindet sich folglich immer eine ***reducirte Form,*** und nur eine.

Das eben gefundene Resultat läfst sich auch so aussprechen: ***dafs unter Voraussetzung einer eigentlichen Darstellung α, β, γ der Zahl a durch die Form G immer eine und nur eine zu a gehörige reducirte Form aufgestellt werden könne, welche der Form G aequivalent ist, und in welche G durch eine Substitution übergeht, deren drei erste Coëfficienten resp. α, β, γ sind.***

Umgekehrt: ***wenn die Form G irgend einer zu a gehörigen reducirten Form R aequivalent ist, so liefert jede Transformation, welche G in R übergehen läfst, eine Darstellung der Zahl a durch die Form G, indem man die Variabeln der Form G den drei ersten Coëfficienten dieser Transformation resp. gleich setzt; und alle Darstellungen, welche man auf diese Weise aus Substitutionen von G in R ableiten kann, sind verschieden.***

In der That: wenn z. B. G durch die Substitution (1.) in R übergeht, so überzeugt man sich durch die Transformation, dafs der erste Coëfficient von R genau demjenigen Werthe gleich wird, welchen G annimmt, wenn man für ihre Variabeln die Werthe resp. α, β, γ setzt; der erste Coëfficient von R ist aber nach der Voraussetzung $= a$, folglich liefern α, β, γ, d. h. die drei ersten Coëfficienten der Substitution wirklich eine Darstellung der Zahl a durch die Form G. Wäre es ferner möglich, dafs sich unter den Darstellungen, welche man auf diese Weise aus den verschiedenen Transformationen von G in R ableiten kann, zwei identische befänden, so müfste es zwei verschiedene Systeme geben, in denen die drei ersten Coëfficienten des einen resp. den drei ersten Coëfficienten des andern gleich sind, und welche beide die Form G in die Form R übergehen lassen. Dies widerstreitet aber dem oben Bewiesenen, nach welchem unter den unendlich vielen, in der Zusammensetzung der Systeme (7.), (8.) enthaltenen Systemen ***nur ein einziges*** existirt, durch welches man zu einer ***reducirten*** Form gelangen kann. Da α, β, γ keinen gemeinschaftlichen Theiler haben können, weil sonst die Determinante der Transformationssysteme nicht der Einheit gleich sein könnte, so sind alle so gefundenen Darstellungen ***eigentliche.***

Alle Darstellungen, welche man auf diese Weise aus einer bestimmten, der Form G aequivalenten reducirten Form R ableiten kann, indem man alle Substitutionen von G in R aufsucht, bilden *eine Gruppe zu der reducirten Form R gehöriger Darstellungen.*

Nach dem bisher Erörterten läfst sich folgende allgemeine Regel zur Auffindung aller eigentlichen Darstellungen einer gegebenen positiven Zahl a durch eine vorgelegte associirte Form G aufstellen.

„Man suche alle reducirten Formen mit dem ersten Coëfficienten a, welche „der Form G aequivalent sind; dieselben seien

$$R, \quad R', \quad R'', \quad \ldots .$$

„Man bestimme alle möglichen Transformationen von G in R; die drei „ersten Coëfficienten jeder dieser Transformationen (die erste Vertical- „reihe) liefern eine Darstellung von a durch G. Man bestimme darauf „alle möglichen Transformationen von G in R'; die drei ersten Coëffi- „cienten jeder dieser Transformationen liefern eine Darstellung; und so „weiter fort, bis man alle der G aequivalenten reducirten Formen er- „schöpft hat; andere eigentliche Darstellungen, als die so gefundenen, „kann es nicht geben."

Alle diese Darstellungen sind verschieden; denn für Darstellungen derselben Gruppe ist dies schon bewiesen; und Darstellungen verschiedener Gruppen können eben so wenig identisch sein, weil es sonst zwei Substitutionen mit denselben drei ersten Coëfficienten gäbe, durch welche G in *zwei* verschiedene *reducirte* Formen überginge; was dem oben Bewiesenen widerstreitet.

Die Darstellung der Zahlen hängt von der Auffindung der reducirten Formen und von der Transformation der Formen ab. Diese beiden Gegenstände werden wir in den beiden folgenden Paragraphen behandeln.

§. 7.

I. „Durch jede gegebene associirte Form können immer Zahlen dargestellt werden, welche zu einer beliebig gegebenen Zahl K relative Primzahlen sind."

Beweisen wir zuerst, dafs man in jeder binären cubischen Form

$$kx^3 + 3lx^2y + 3mxy^2 + ny^3$$

den Variabeln x, y solche reelle ganze Werthe geben kann, dafs der Werth der Form durch eine gegebene Primzahl q nicht theilbar wird: vorausgesetzt,

dafs k, $3l$, $3m$, n nicht alle vier durch q theilbar und dafs nicht zugleich k und n gerade, l und m ungerade sind, wenn $q=2$ genommen wird.

Für $q=2$ ist entweder einer der äufsersten Coëfficienten z. B. k ungerade; dann nehme man $x=1$, $y=0$: oder beide äufsere Coëfficienten k und n sind gerade; in diesem Falle ist nothwendig eine der beiden Zahlen l und m gerade, die andern sind ungerade; also nehme man $x=1$, $y=1$.

Für $q=3$ können k und n nicht beide durch 3 theilbar sein. Ist k durch 3 theilbar, so nehme man $x=0$, $y=1$: ist n durch 3 theilbar, so nehme man $x=1$, $y=0$; und sind k und n beide nicht durch 3 theilbar, so passen beide Systeme.

Für $q>3$ ist entweder einer (oder auch beide) der beiden äufsern Coëfficienten z. B. k nicht durch q theilbar; dann nehme man $x=1$, $y=0$, und der Werth der Form wird nicht durch q theilbar sein: oder k und n sind beide durch q theilbar; in diesem zweiten Falle können l und m nicht beide durch q theilbar sein. Es sei l z. B. nicht durch q theilbar, m mag übrigens durch q theilbar sein, oder nicht. Da das erste und vierte Glied der Form für jeden Werth der Variabeln durch q theilbar ist, so kommt Alles darauf an, die Variabeln so zu bestimmen, dafs das Product der drei Factoren

$$x.y(lx+my)$$

nicht $\equiv 0$ (mod. q) wird. Da l nicht durch q theilbar ist, so giebt es unter den q^2 Systemen, welche man erhält, wenn man x und y beide alle Werthe der Reihe

$$0,\ 1,\ 2,\ 3,\ \ldots\ q-1$$

durchlaufen läfst, nur q Systeme, für welche der Ausdruck $lx+my$ durch q theilbar wird; denn für jedes gegebene y genügt der Congruenz $lx+my\equiv 0$ (mod. q) nur ein einziges x; unter den q^2 Systemen giebt es also q^2-q solche, für welche $lx+my$ nicht durch q theilbar ist. Von der andern Seite befinden sich unter den q^2 Systemen überhaupt nur $2q-1$ Systeme, für welche einer der beiden Variabeln, oder beide $\equiv 0$ (mod. q) sind: aber $q^2>3q$, folglich um so mehr $q^2-q>2q-1$; mithin bleiben immer noch Systeme übrig, für welche alle drei Factoren x, y, $lx+my$, also ihr Product nicht durch q theilbar sind.

Es sei jetzt F eine gegebene associirte Form und ihre Variabeln u, v, w seien so zu bestimmen, dafs F nicht durch die Primzahl q theilbar wird. Aus der Form F kann man drei binäre cubische Formen mit den Variabeln resp. v, w; u, w; u, v bilden, wenn man nach und nach erst $u=0$, dann

$v=0$, dann $w=0$ setzt. Es sind zwei Fälle möglich: entweder sind wenigstens in einer dieser drei binären Formen nicht alle vier Coëfficienten durch q theilbar, oder in allen dreien sind sämmtliche Coëfficienten durch q theilbar; in diesem zweiten Falle ist nothwendig der Coëfficient von uvw nicht durch q theilbar, denn sonst würden alle 10 Coëfficienten der associirten Form den gemeinschaftlichen Theiler q haben; also braucht man nur $u=v=w=1$ zu nehmen und es ist dann $F\equiv$ dem Coëfficienten von uvw (mod. q), also nicht durch q theilbar; wie verlangt wird. In dem ersten Falle nehme man diejenige von den drei binären Formen, oder eine von denjenigen, für welche nicht alle vier Coëfficienten durch q theilbar sind und bestimme nach dem Obigen die Werthe ihrer beiden Variabeln dergestalt, dafs der Werth der binären Form nicht durch q theilbar wird; die dritte Variable der associirten Form setze man $=0$, so wird der Werth der ganzen associirten Form dem der binären Form gleich, also ebenfalls nicht durch q theilbar sein. Für den Fall $q=2$ ist namentlich zu bemerken, dafs unter den drei binären Formen immer nothwendig wenigstens eine ist, in welcher nicht zugleich beide äufsern Coëfficienten gerade und beide mittlern Coëfficienten ungerade sind, weil sonst die associirte Form F eine *uneigentliche* wäre, welche von den Untersuchungen ausgeschlossen wurde; also kann man auch für diesen speciellen Fall $q=2$ wenigstens eine der drei binären Formen durch q nicht-theilbar, nämlich ungerade machen.

Setzt man nun $K=q^n q'^{n'} q''^{n''}\ldots$, wo $q, q', q'', \ldots$ verschiedene Primzahlen sind, und bezeichnet durch α, β, γ; α', β', γ'; $\alpha'', \beta'', \gamma''$; etc. etc. Systeme von Werthen von u, v, w, für welche resp. F nicht durch q, F nicht durch q', F nicht durch q'' theilbar ist, u. s. w., so darf man nur zu gleicher Zeit u den Zahlen $\alpha, \alpha', \alpha'', \ldots$ resp. nach den Moduln $q, q', q'', \ldots$, $v\equiv\beta, \beta', \beta'', \ldots$, $w\equiv\gamma, \gamma', \gamma'', \ldots$ resp. nach denselben Moduln congruent setzen, was nach *Disq. arithm.* 33. immer möglich ist; für solche Werthe von u, v, w wird der Werth der Form F weder durch q, noch durch q', noch durch q'' u. s. w. theilbar, folglich zu K relative Primzahl sein. Es läfst sich immer annehmen, dafs die Darstellung eine *eigentliche* ist, denn im entgegengesetzten Falle braucht man nur mit dem Cubus des gröfsten gemeinschaftlichen Theilers von u, v, w zu dividiren.

II. „Wenn $I, K, L, I', K', L', I'', K'', L''$ neun ganze Zahlen sind, q eine Primzahl >3 ist, und in dem entwickelten und nach Potenzen und Producten der Variabeln geordneten Producte der drei Linearfactoren

$$(10.)\quad (Iu+Kv+Lw)(I'u+K'v+L'w)(I''u+K''v+L''w)$$

sämmtliche 10 Coëfficienten durch q^n theilbar sind, so kann dies nicht anders geschehen, als wenn die n Factoren q sich dergestalt auf die drei Linearfactoren vertheilen, dafs in dem ersten alle drei Coëfficienten I, K, L durch q^α, in dem zweiten alle drei Coëfficienten I', K', L' durch q^β, in dem dritten alle drei Coëfficienten I'', K'', L'' durch q^γ theilbar sind, und dafs

$$\alpha+\beta+\gamma=n$$

ist; wobei übrigens eine oder zwei von den ganzen Zahlen α, β, γ der Null gleich sein können."

In einem Ausdrucke von der Form $Iu+Kv+Lw$, dessen Coëfficienten nicht alle drei durch q theilbar sind, giebt es unter den q^3 Systemen u, v, w, welche man erhält, wenn man jede der drei Variabeln die Glieder der Reihe

$$0,\ 1,\ 2,\ 3,\ \ldots\ q-1$$

durchlaufen läfst, und deren Inbegriff wir durch Ω bezeichnen, nur q^2 solche, für welche dieser Ausdruck $\equiv 0 \pmod{q}$ wird; denn zu jedem gegebenen Werthe von v und w, deren q^2 sind, giebt es, wenn z. B. I nicht durch q theilbar ist, nur einen einzigen Werth von u, der den Ausdruck $\equiv 0 \pmod{q}$ macht; oder wenn K nicht durch q theilbar ist, so giebt es zu jedem Werthenpaare von u und w nur einen Werth von v; oder wenn L nicht durch q theilbar ist, so giebt es zu jedem Werthenpaare u, v nur ein zugehöriges w.

Hiernach behaupte ich zuerst, dafs, unter der in dem Lehrsatze gemachten Voraussetzung, wenigstens von einem der drei Factoren (10.) die drei Coëfficienten durch q theilbar sein werden. In der That, wäre dies nicht der Fall, so könnte es für jeden der drei Factoren (10.) unter den Systemen Ω nur q^2 solche geben, welche ihn durch q theilbar machen; also könnte es überhaupt höchstens $3q^2$ solche geben, für welche irgend einer dieser drei Factoren $\equiv 0 \pmod{q}$ wird; mithin gäbe es höchstens $3q^2$ Systeme unter denen Ω, welche das Product der drei Factoren (10.) $\equiv 0 \pmod{q}$ machen. Von der andern Seite wird aber dies Product für alle q^3 Systeme Ω durch q theilbar, da nach der Voraussetzung seine sämmtlichen Coëfficienten $\equiv 0 \pmod{q}$ sind: also müfste nothwendig

$$3q^2 \geqq q^3$$

sein; was der Voraussetzung $q > 3$ widerstreitet.

Da also nothwendig in einem von den drei Linearfactoren in (10.) alle Coëfficienten durch q theilbar sind, so dividire man in demselben die letzteren durch q weg und schreibe den auf diese Weise erhaltenen Ausdruck an die

Stelle des alten. In dem Producte der drei Factoren, welche sich nach dieser Operation finden, werden immer noch offenbar alle 10 Coëfficienten durch q^{n-1} theilbar sein; es wird also wieder einer der drei Factoren seine drei Coëfficienten durch q theilbar haben; dividirt man sie durch q weg und setzt den neuen Ausdruck an die Stelle des alten, so werden in dem Product der drei Ausdrücke, welche man jetzt erhält, alle 10 Coëfficienten noch durch q^{n-2} theilbar sein; folglich wird wieder einer der drei Factoren seine drei Coëfficienten durch q theilbar haben, welche man abermals durch q wegdividiren kann; und so weiter. Setzt man diese Operation fort, bis alle n Factoren q erschöpft sind, so werden sich, wie leicht zu sehen, diese n Factoren q wirklich in der Weise auf die drei Linearfactoren (10.) vertheilen müssen, wie es der Lehrsatz behauptet. In der That liefert jeder Schritt dieser Operation für einen der drei Ausdrücke (10.) einen entsprechenden Factor q: entsprechen also diesen drei Ausdrücken resp. α, β, γ Factoren q, so ist $\alpha+\beta+\gamma=n$, weil die Operation aus n Schritten besteht.

Dehnt man den so eben für Potenzen von Primzahlen bewiesenen Satz auf zusammengesetzte Zahlen mit mehreren Primfactoren aus, indem man ihn für jeden Primfactor besonders anwendet, so lautet er wie folgt.

„Wenn von dem Product der drei Linearfactoren in (10.) die sämmtlichen 10 Coëfficienten durch

$$a = q^n q'^{n'} q''^{n''} \dots$$

theilbar sind, wo q, q', q'', ... verschiedene Primzahlen >3 bedeuten, so ist die allgemeinste Annahme, die man machen kann,

$$\begin{aligned} &I,\ K,\ L \text{ durch } q^{\alpha} q'^{\alpha'} q''^{\alpha''} \dots, \\ &I',\ K',\ L' \text{ durch } q^{\beta} q'^{\beta'} q''^{\beta''} \dots, \\ &I'',\ K'',\ L'' \text{ durch } q^{\gamma} q'^{\gamma'} q''^{\gamma''} \dots \end{aligned}$$

theilbar zu setzen, während

$$\alpha+\beta+\gamma=n, \quad \alpha'+\beta'+\gamma'=n', \quad \alpha''+\beta''+\gamma''=n'', \text{ etc. ist."}$$

III. „Für jede reelle ganze Zahl a, welche zu $3p$ relative Primzahl ist, und deren sämmtliche *complexe* Primfactoren δ, δ', δ'', ... den Bedingungen

$$\left[\frac{pp_1}{\delta}\right]=1, \quad \left[\frac{pp_1}{\delta'}\right]=1, \quad \left[\frac{pp_1}{\delta''}\right]=1, \text{ etc.},$$

also auch den Bedingungen

$$\left[\frac{pp_2}{\delta}\right]=1, \quad \left[\frac{pp_2}{\delta'}\right]=1, \quad \left[\frac{pp_2}{\delta''}\right]=1, \text{ etc.}$$

genügen, lassen sich zwei *conjugirte* complexe Zahlen ζ_1 und ζ_2 finden, welche

die drei Congruenzen

$$\zeta_1^3 \equiv pp_1, \quad \zeta_2^3 \equiv pp_2, \quad \zeta_1\zeta_2 \equiv p \pmod{a}$$

befriedigen."

Man sieht leicht ein, dafs die Richtigkeit unseres Satzes im Allgemeinen, d. h. für irgend einen Werth von a, von der des speciellen Falles abhängt, wenn a Potenz einer reellen Primzahl ist; denn wenn a und a' zwei reelle Zahlen ohne gemeinschaftlichen Theiler sind, und

$$\zeta_1^3 \equiv pp_1, \quad \zeta_2^3 \equiv pp_2, \quad \zeta_1\zeta_2 \equiv p \pmod{a} \text{ und}$$
$$\zeta_1'^3 \equiv pp_1, \quad \zeta_2'^3 \equiv pp_2, \quad \zeta_1'\zeta_2' \equiv p \pmod{a'}$$

ist, wo ζ_1 mit ζ_2 und ζ_1' mit ζ_2' conjugirt ist, so braucht man nur ζ_1'' so anzunehmen, dafs sie zugleich $\equiv \zeta_1 \pmod{a}$ und $\equiv \zeta_1' \pmod{a'}$ wird, und ζ_2'' der conjugirten Zahl von ζ_1'' gleich zu setzen, so dafs, weil a, a' reell sind, ζ_2'' zugleich $\equiv \zeta_2 \pmod{a}$ und $\equiv \zeta_2' \pmod{a'}$ wird, und man wird

$$\zeta_1''^3 \equiv pp_1 \pmod{aa'}, \quad \zeta_2''^3 \equiv pp_2 \pmod{aa'}, \quad \zeta_1''\zeta_2'' \equiv p \pmod{aa'}$$

haben; also läfst sich der Gegenstand immer auf Potenzen reeller Primzahlen zurückführen.

Es sei q eine von p verschiedene reelle Primzahl > 3, und $a = q^n$. Es sei zuerst $q \equiv 2 \pmod{3}$, also q zugleich complexe Primzahl. Da $\left[\frac{pp_1}{q}\right] = 1$ ist, so existirt eine complexe Zahl ζ_1, für welche $\zeta_1^3 \equiv pp_1 \pmod{q^n}$ ist (Vergl. „Beweis des Reciprocitätssatzes für die cubischen Reste. §. 2." im 27ten Bande dieses Journals), und man kann durch Hinzufügung von Vielfachen des Moduls den Fall immer so einrichten, dafs ζ_1 zu p relative Primzahl ist *). Bedeutet ζ_2 die der ζ_1 conjugirte Zahl, so hat man auch, da q^n reell ist, $\zeta_2^3 \equiv pp_2 \pmod{q^n}$. Aus den beiden eben geschriebenen Congruenzen folgt durch Multiplication, wenn man $\zeta_1\zeta_2 = \psi$ setzt, so dafs $\psi = N(\zeta_1)$ *reell* ist, $\psi^3 \equiv p^3 \pmod{q^n}$, oder

$$(\psi - p)(\psi^2 + p\psi + p^2) \equiv 0 \pmod{q^n}.$$

Der zweite Factor, welcher eine quadratische Form mit der Determinante -3 ist, kann nicht durch die Primzahl q von der Form $3m+2$ theilbar sein; mithin ist nothwendig $\psi \equiv p \pmod{q^n}$, d. h. $\zeta_1\zeta_2 \equiv p \pmod{q^n}$.

Es sei zweitens $q \equiv 1 \pmod{3}$ und $q = \delta_1\delta_2$, wo δ_1, δ_2 conjugirte complexe Primzahlen sind. Da

---

*) Man findet zunächst ζ_1 so, dafs $\zeta_1^3 \equiv pp_1 \pmod{q}$ ist, und dann steigt man nach einer bekannten Methode zu den höhern Potenzen des Moduls auf. (Vergl. *Gauss*, Disq. arithm. 88, 101, oder *Dirichlet*, Recherches sur les formes quadr. §. 9.)

$$\left[\frac{pp_1}{\delta_1}\right] = 1 \quad \text{und} \quad \left[\frac{pp_1}{\delta_2}\right] = 1$$

ist, so läfst sich den beiden Congruenzen

$$x^3 \equiv pp_1 \pmod{\delta_1^n}, \qquad x'^3 \equiv pp_1 \pmod{\delta_2^n}$$

genügen; und zwar durch reelle Werthe von x und x'. Diese beiden Congruenzen geben, wenn man überall ρ mit ρ^2 vertauscht, noch die beiden folgenden:

$$x^3 \equiv pp_2 \pmod{\delta_2^n}, \qquad x'^3 \equiv pp_2 \pmod{\delta_1^n}.$$

Multiplicirt man die erste mit der vierten und setzt $xx' = \psi$, so ergiebt sich

$$\psi^3 \equiv p^3 \pmod{\delta_1^n}, \quad \text{oder} \quad (\psi - p)(\psi - \rho p)(\psi - \rho^2 p) \equiv 0 \pmod{\delta_1^n}.$$

Von diesen drei Factoren können nicht zwei zugleich durch δ_1 theilbar sein, weil sonst auch ihre Differenz $(1-\rho)p$ oder $(1-\rho^2)p$ oder $(\rho-\rho^2)p$ durch δ_1 theilbar wäre, der über q gemachten Voraussetzung zuwider: also ist nothwendig einer der drei Factoren durch den ganzen Modul δ_1^n theilbar, und man wird x und x' immer so annehmen können, dafs dies der *erste* ist; denn da ρ und ρ^2 selbst reellen Zahlen nach dem Modul δ_1^n congruent sind, so kann man, wenn die gefundenen Werthe von x und x' nicht schon den ersten Factor $\psi - p$ durch δ_1^n theilbar machen, dies dadurch bewirken, dafs man an die Stelle von x' die der complexen Zahl $\rho^2 x'$, oder die der complexen Zahl $\rho x'$ congruente reelle Zahl setzt. Wählt man, nachdem dies geschehen, eine complexe Zahl ζ_1, welche zugleich $\equiv x \pmod{\delta_1^n}$ und $\equiv x' \pmod{\delta_2^n}$ ist, und nimmt für ζ_2 ihre conjugirte Zahl, so werden die drei Congruenzen

$$\zeta_1^3 \equiv pp_1 \pmod{q^n}, \qquad \zeta_2^3 \equiv pp_2 \pmod{q^n}, \qquad \zeta_1\zeta_2 \equiv p \pmod{q^n}$$

erfüllt werden. In der That ist $\zeta_1 \equiv x \pmod{\delta_1^n}$, also $\zeta_1^3 \equiv x^3 \equiv pp_1 \pmod{\delta_1^n}$, und $\zeta_1 \equiv x' \pmod{\delta_2^n}$, also $\zeta_1^3 \equiv x'^3 \equiv pp_1 \pmod{\delta_2^n}$; folglich ist die Differenz $\zeta_1^3 - pp_1$ durch die beiden relativen Primzahlen δ_1^n und δ_2^n, mithin auch durch ihr Product q^n theilbar. Ferner hat man, da ζ_2 zu ζ_1 conjugirt und x, x' reell, also sich selbst conjugirt sind,

$$\zeta_2 \equiv x \pmod{\delta_2^n}, \qquad \zeta_2 \equiv x' \pmod{\delta_1^n},$$

folglich

$$\zeta_2^3 \equiv x^3 \equiv pp_2 \pmod{\delta_2^n}, \qquad \zeta_2^3 \equiv x'^3 \equiv pp_2 \pmod{\delta_1^n},$$

mithin auch

$$\zeta_2^3 \equiv pp_2 \pmod{q^n}.$$

Endlich hat man $\zeta_1\zeta_2 \equiv xx' \pmod{\delta_1^n}$, also $\zeta_1\zeta_2 \equiv \psi \equiv p \pmod{\delta_1^n}$: aber $\zeta_1\zeta_2$ und p sind reell, folglich kann die Differenz $\zeta_1\zeta_2 - p$ nicht anders durch δ_1^n theilbar sein, als wenn sie zugleich durch q^n theilbar ist; was zu beweisen war.

Es würde nicht schwer sein, die Anzahl der Auflösungen der Congruenzen zu bestimmen; aber da die Kenntnifs dieser Anzahl keinen Vortheil für unsern Zweck hat, so übergeben wir ihre Bestimmung der Kürze wegen und wenden uns zu dem Hauptgegenstande dieses Paragraphen, der Auffindung der reducirten Formen.

IV. Die bisherigen Untersuchungen dieses Paragraphen führen zu der Lösung des folgenden wichtigen Problems:

Alle reducirten Formen zu finden, deren erster Coëfficient a eine gegebene positive ganze Zahl ist, die mit $2(pp_1-pp_2)$ keinen gemeinschaftlichen Theiler hat.

Es sei allgemein F' irgend eine associirte Form mit dem ersten Coëfficienten a. Man setze

$$(11.)\quad a^2F' = (au+\lambda v+\lambda' w)(au+\mu v+\mu' w)(au+\nu v+\nu' w),$$

$\lambda = b+(c+d\varrho)\eta+(c+d\varrho^2)\vartheta,\quad \lambda' = b'+(c'+d'\varrho)\eta+(c'+d'\varrho^2)\vartheta$ u. s. w., wie in §. 6., während

$$(12.)\quad b,\ c,\ d,\ b',\ c',\ d'$$

reelle ganze Zahlen sind, die der Bedingung

$$(13.)\quad cd'-c'd = a$$

genügen. Das Problem verlangt offenbar nichts anders, als die ganzen Zahlen (12.) auf alle möglichen Arten so zu bestimmen, dafs

1) in dem entwickelten und geordneten Producte der drei Factoren auf der rechten Seite in (11.) alle 10 Coëfficienten den gröfsten gemeinschaftlichen Theiler a^2 haben (*A.*),
2) dafs die Bedingung (13.) erfüllt wird (*B.*) und
3) dafs den Bedingungen (9.) genügt wird, nemlich dafs

$$(9.)\quad 0\leqq b<a,\quad c=t,\quad 0\leqq d<t',\quad 0\leqq b'<a,\quad c'=0,\quad d'=t'$$

ist, während tt' jede mögliche Zerfällung der Zahl a in das Product zweier Factoren vorstellen kann (*C*).

Berücksichtigen wir zuerst hauptsächlich die Bedingung (*A.*). Da in dem entwickelten Producte der drei Factoren (11.) alle Coëfficienten durch a^2 theilbar sein sollen, so wird dies namentlich auch von den Coëfficienten von v^3 und w^3 gelten, welche folgende sind:

$$(14.)\quad \begin{cases} b^3+pp_1(c+d\varrho)^3+pp_2(c+d\varrho^2)^3-3pb(c+d\varrho)(c+d\varrho^2), \\ b'^3+pp_1(c'+d'\varrho)^3+pp_2(c'+d'\varrho^2)^3-3pb'(c'+d'\varrho)(c'+d'\varrho^2). \end{cases}$$

Es sei q irgend ein reeller Primfactor von a und q^n sei die höchste in a aufgehende Potenz von q, so werden die beiden Ausdrücke in (14.) durch

q^{2n} theilbar sein. Da wegen der Gleichung (13.) die höchste in die vier Zahlen c, d, c', d' zugleich aufgehende Potenz von q nothwendig $\leqq \sqrt{q^n}$ sein mufs, so wird entweder für die beiden Zahlen c, d, oder für die beiden Zahlen c', d' die höchste in beide aufgehende Potenz von q nothwendig $\leqq \sqrt{q^n}$ sein. Es sei dies z. B. für die beiden Zahlen c und d der Fall; dann wird um so mehr die höchste Potenz von q, welche in die drei Zahlen b, c, d zugleich aufgeht und welche wir durch q^μ bezeichnen, $\leqq \sqrt{q^n}$ sein. Dividirt man folglich die erste der beiden Formen (14.) durch $q^{3\mu}$, welches $\leqq \sqrt{q^{3n}}$ also gewifs $< q^{2n}$ ist, und durch die Cuben der übrigen gemeinschaftlichen Factoren von b, c, d fort, so wird die nach dieser Operation übrig bleibende Form immer noch durch q theilbar sein. Hätte man angenommen, dafs für c', d' die höchste Potenz von q, welche beide theilt, $\leqq \sqrt{q^n}$ sei, so würde man dasselbe Resultat für die zweite Form (14.) erhalten. Wir schliefsen hieraus nach §. 3., dafs die Primzahl q ein Theiler der Form Φ sein mufs und dafs folglich für jeden complexen Primfactor δ von a die Bedingung

$$(15.)\qquad \left[\frac{pp_1}{\delta}\right] = \left[\frac{pp_2}{\delta}\right] = 1,$$

oder, was nach dem cubischen Reciprocitätssatze dasselbe besagt, dafs für jeden reellen Primfactor q von a die Bedingung

$$(16.)\qquad \left[\frac{q}{p_1}\right] = 1 \text{ erfüllt werden mufs.}$$

Wenn also nicht für jeden Primfactor von a die Bedingungen (15.), (16.) *erfüllt werden, so giebt es gar keine zu a gehörigen reducirten Formen.*

Nehmen wir also an, dafs die Zahl a allen in der Gleichung (15.) oder (16.) enthaltenen Bedingungen genügt. Da jeder complexe Primfactor δ von a der Gleichung (15.) genügt, so lassen sich nach III. zwei conjugirte complexe Zahlen ζ_1 und ζ_2 finden, welche die drei Congruenzen

$$(17.)\qquad \zeta_1^3 \equiv pp_1,\quad \zeta_2^3 \equiv pp_2,\quad \zeta_1\zeta_2 \equiv p \pmod{a^3}$$

erfüllen. Setzt man der Kürze wegen

$$\begin{aligned} au+bv+b'w &= U,\\ cv+c'w &= V,\\ dv+d'w &= W,\end{aligned}$$

$$V+W\varrho = Y,\quad V+W\varrho^2 = Z,$$

so nimmt das entwickelte Product der drei Factoren in (11.) die Form

$$(18.)\qquad (U+Y\eta+Z\vartheta)(U+Y\varrho\eta+Z\varrho^2\vartheta)(U+Y\varrho^2\eta+Z\varrho\vartheta) = U^3+pp_1Y^3+pp_2Z^3-3pUYZ$$

an. Wegen der Congruenzen (17.) ist dieser Ausdruck (18.) congruent dem folgenden Ausdrucke (mod. a^3)

$$(19.)\quad U^3+\zeta_1^3 Y^3+\zeta_2^3 Z^3-3\,U\zeta_1 Y\zeta_2 Z,$$

unabhängig von den Werthen, welche man den Variabeln u, v, w giebt; und ordnet man sowohl (18.) als (19.) nach u, v, w, so werden in diesen beiden Ausdrücken je zwei entsprechende Coëfficienten nach dem Modul a^3 congruent sein. Da nun alle zehn Coëfficienten des geordneten Ausdrucks (18.) durch a^2 theilbar sein sollen, so ist es nöthig und hinreichend, dafs dasselbe auch für den Ausdruck (19.) der Fall ist; der Ausdruck (19.) ist gleich dem Producte der drei reellen und *rationalen* Factoren

$$(20.)\quad (U+Y\zeta_1+Z\zeta_2)(U+Y\varrho\zeta_1+Z\varrho^2\zeta_2)(U+Y\varrho^2\zeta_1+Z\varrho\zeta_2),$$

folglich ist es nöthig und hinreichend, dafs in dem entwickelten und nach u, v, w geordneten Producte der drei Factoren (20.) alle zehn Coëfficienten durch a^2 theilbar sind. Das Problem ist also jetzt darauf zurückgeführt, die ganzen Zahlen (12.) auf alle möglichen Arten so zu bestimmen, dafs in dem entwickelten und nach den Variabeln u, v, w geordneten Producte (20.) alle zehn Coëfficienten durch a^2 theilbar sind und dafs die Bedingungen (B.) und (C.) erfüllt werden. Die Bedingung, dafs a^2 nicht blofs gemeinschaftlicher Theiler, sondern gröfster gemeinschaftlicher Theiler der Coëfficienten des entwickelten Productes (11.) sein soll, wird dann schon von selbst erfüllt; wie wir später sehen werden.

V. Da in dem nach u, v, w geordneten Producte (20.), welches wir durch

$$(21.)\quad (au+Kv+Lw)(au+K'v+L'w)(au+K''v+L''w)$$

bezeichnen und wo

$$\begin{aligned}
K &= b+(c+d\varrho)\zeta_1+(c+d\varrho^2)\zeta_2; & L &= b'+(c'+d'\varrho)\zeta_1+(c'+d'\varrho^2)\zeta_2;\\
&= b+c(\zeta_2+\zeta_2)+d(\varrho\zeta_1+\varrho^2\zeta_2); & &= b'+c'(\zeta_1+\zeta_2)+d'(\varrho\zeta_1+\varrho^2\zeta_2);\\
K' &= b+c(\varrho\zeta_1+\varrho^2\zeta_2)+d(\varrho^2\zeta_1+\varrho\zeta_2); & L' &= b'+c'(\varrho\zeta_1+\varrho^2\zeta_2)+d'(\varrho^2\zeta_1+\varrho\zeta_2);\\
K'' &= b+c(\varrho^2\zeta_1+\varrho\zeta_2)+d(\zeta_1+\zeta_2); & L'' &= b'+c'(\varrho^2\zeta_1+\varrho\zeta_2)+d'(\zeta_1+\zeta_2)
\end{aligned}$$

gesetzt wird, alle neun Coëfficienten der drei Factoren reelle ganze Zahlen sind, so schliefsen wir nach II., dafs die allgemeinste Annahme, die man machen kann, damit das Product, entwickelt, alle zehn Coëfficienten durch

$$a^2 = q^{2n}q'^{2n'}q''^{2n''}\ldots.$$

theilbar habe, die folgende ist:

$$(D.)\quad \begin{cases} a,\ K,\ L \text{ theilbar durch } q^{\alpha}q'^{\alpha'}q''^{\alpha''}\ \ldots,\\ a,\ K',\ L' \text{ theilbar durch } q^{\beta}q'^{\beta'}q''^{\beta''}\ \ldots,\\ a,\ K'',\ L'' \text{ theilbar durch } q^{\gamma}q'^{\gamma'}q''^{\gamma''}\ \ldots. \end{cases}$$

wo

$$\alpha+\beta+\gamma = 2n, \quad \alpha'+\beta'+\gamma' = 2n', \quad \alpha''+\beta''+\gamma'' = 2n'' \text{ etc. ist.}$$

Sehen wir, welche Werthe den Exponenten α, β, γ u. s. w. gegeben werden können.

Das lineäre System

$$(22.) \quad \begin{Bmatrix} a, & K, & L \\ a, & K', & L' \\ a, & K'', & L'' \end{Bmatrix}$$

ist offenbar aus den drei Systemen

$$\begin{Bmatrix} 1, & \zeta_1, & \zeta_2 \\ 1, & \varrho\zeta_1, & \varrho^2\zeta_2 \\ 1, & \varrho^2\zeta_1, & \varrho\zeta_2 \end{Bmatrix}, \quad \begin{Bmatrix} 1, & 0, & 0 \\ 0, & 1, & \varrho \\ 0, & 1, & \varrho^2 \end{Bmatrix} \quad \text{und} \quad \begin{Bmatrix} a, & b, & b' \\ 0, & c, & c' \\ 0, & d, & d' \end{Bmatrix}$$

zusammengesetzt, deren Determinanten resp. die folgenden sind:

$$3(\varrho^2-\varrho)\zeta_1\zeta_2; \quad \varrho^2-\varrho; \quad a(cd'-c'd) = a^2:$$

also ist die Determinante des Systems (22.)

$$= -9a^2\zeta_1\zeta_2,$$

folglich die des Systems

$$(23.) \quad \begin{Bmatrix} 1, & K, & L \\ 1, & K', & L' \\ 1, & K'', & L'' \end{Bmatrix}, \quad = -9a\zeta_1\zeta_2.$$

Aber da a zu $2(pp_1-pp_2)$ relative Primzahl und p_1-p_2 durch 3 theilbar ist, so ist auch a zu 9 relative Primzahl. Ebenso ist a zu $\zeta_1\zeta_2$ relative Primzahl; denn wenn es anders wäre, so müfste wegen der dritten der drei Congruenzen (17.) auch p mit a einen gemeinschaftlichen Theiler haben; gegen die Voraussetzung. Die Determinante des Systems (23.) kann also keinen der Primfactoren von a in einer höhern Potenz enthalten, als in welcher derselbe in a vorkommt; also ist diese Determinante durch q^n, $q'^{n'}$ etc. theilbar, aber durch keine höhere Potenz von q, q', etc. Andrerseits erhellet aus dem Bildungsgesetze der Determinante, dafs, wenn z. B. für den Primfactor q, α die gröfste der drei Zahlen α, β, γ, oder wenigstens nicht kleiner als irgend eine von den beiden andern ist, diese Determinante nothwendig durch $q^{\beta+\gamma}$ theilbar sein mufs. In der That enthält diese Determinante sechs Glieder, von denen jedes aus drei Factoren besteht, nemlich aus einer Einheit, aus einer der Horizontalreihen genommen, aus einem K (K', K'') und einem L (L', L''), aus den beiden andern Verticalreihen genommen. Jedes der 6 Glie-

der mufs also durch eine der drei Potenzen

$$q^{\alpha+\beta},\quad q^{\alpha+\beta},\quad q^{\beta+\gamma}$$

theilbar sein. Da nun $q^{\beta+\gamma}$ die kleinste der drei Potenzen ist, so theilt die letztere die beiden andern, folglich alle sechs Glieder der Determinante. Es folgt hieraus und aus dem vorhin Bemerkten:

$$\beta+\gamma \leqq n.$$

Von der andern Seite ist $\alpha \leqq n$, weil α durch q^{α} theilbar ist; und aus der zuerst geschriebenen Ungleichung folgt $\alpha+\beta+\gamma \leqq \alpha+n$, also, wegen $\alpha+\beta+\gamma = 2n$, $2n \leqq \alpha+n$, $n \leqq \alpha$. Es mufs also zugleich $n \geqq \alpha$ und $n \leqq \alpha$ sein, welches

$$\alpha = n$$

erfordert. *Unter den drei Zahlen α, β, γ ist demnach nothwendig eine $= n$, während die Summe der beiden andern ebenfalls $= n$ ist.* Ebenso wird bewiesen, dafs unter den Zahlen α', β', γ' nothwendig eine $= n'$ und die Summe der beiden andern $= n'$ ist; und so weiter (*E.*).

Durch die Bedingung (*E.*) wird die Anzahl der möglichen Combinationen bedeutend beschränkt. Ich behaupte aber jetzt, dafs alle diese Combinationen α, β, γ; α', β', γ'; etc., welche der Bedingung (*E.*) genügen, in (*D.*) wirklich vorkommen können und dafs jeder derselben *eine* und *nur eine reducirte Form* entspricht.

VI. Um diese Behauptung zu beweisen, wollen wir die Werthe $c = t$, $c' = 0$, $d' = t'$ aus (9.) in die Ausdrücke für K, L u. s. w. einführen. Man erhält dadurch

$$(24.)\quad \begin{cases} K\; = b + t(\zeta_1 + \zeta_2) + d(\varrho\zeta_1 + \varrho^2\zeta_2), & L\; = b' + t'(\varrho\zeta_1 + \varrho^2\zeta_2), \\ K' = b + t(\varrho\zeta_1 + \varrho^2\zeta_2) + d(\varrho^2\zeta_1 + \varrho\zeta_2), & L' = b' + t'(\varrho^2\zeta_1 + \varrho\zeta_2), \\ K'' = b + t(\varrho^2\zeta_1 + \varrho\zeta_2) + d(\zeta_1 + \zeta_2), & L'' = b' + t'(\zeta_1 + \zeta_2); \end{cases}$$

und alles kommt darauf an, zu zeigen, dafs es immer ein, und nur ein System von Werthen b, b', t, t', d giebt, für welche b und b' in der Reihe

$$0,\ 1,\ 2,\ 3,\ \ldots\ a-1$$

liegen, $tt' = a$ ist, d in der Reihe

$$0,\ 1,\ 2,\ 3,\ \ldots\ t'-1$$

liegt, und für welche den Congruenzen

$$\begin{aligned} K &\equiv L \equiv 0 \pmod{q^{\alpha} q'^{\alpha'} q''^{\alpha''} \ldots}, \\ K' &\equiv L' \equiv 0 \pmod{q^{\beta} q'^{\beta'} q''^{\beta''} \ldots}, \\ K'' &\equiv L'' \equiv 0 \pmod{q^{\gamma} q'^{\gamma'} q''^{\gamma''} \ldots} \end{aligned}$$

genügt wird, wo α, β, γ irgend eine gegebene Combination von (nicht negati-

ven) ganzen Zahlen ist, von denen eine $= n$ und die Summe der beiden andern ebenfalls $= n$ ist, ferner α', β', γ' irgend eine gegebene Combination von ganzen Zahlen ist, von denen eine, und die Summe der beiden andern $= n'$, u. s. w.

Unter der grofsen Anzahl von Fällen, welche sich hier unterscheiden lassen, wollen wir einen *ad libitum* nehmen, welcher das beste Licht über den Gegenstand verbreiten kann; es wird dann leicht sein, nach diesem Muster die Untersuchung für die übrigen Fälle anzustellen.

Es seien drei Primzahlen q, q', q'' vorhanden. Von den drei Exponenten α, β, γ sei α der kleinste, $\gamma = n$ und $\alpha + \beta = n$; von den drei Exponenten α', β', γ' sei β' der kleinste, $\alpha' = n'$, $\beta' + \gamma' = n'$; von den drei Exponenten $\alpha'', \beta'', \gamma''$ sei γ'' der kleinste, $\beta'' = n''$, $\alpha'' + \gamma'' = n''$. Dies ist einer der Fälle, welche die gröfste Mannigfaltigkeit darbieten.

Löset man die drei Gleichungen für K, K', K'' nach b, t, d, als den Unbekannten, nach der bekannten Methode der Determinante auf, so erhält man, da $-9\zeta_1\zeta_2$ die Determinante des Systems ist,

$$-9\zeta_1\zeta_2 b, \quad -9\zeta_1\zeta_2 t, \quad -9\zeta_1\zeta_2 d$$

als lineäre Functionen von K, K', K'' mit ganzen Coëfficienten ausgedrückt. Da nun $-9\zeta_1\zeta_2$ relative Primzahl zu a ist, so wird jeder in a aufgehende gemeinschaftliche Theiler von K, K', K'' in b, t, d zugleich aufgehen. Da von der andern Seite q^α die kleinste unter den drei Potenzen q^α, q^β, q^n ist, also alle drei theilt, da $q'^{\beta'}$ die kleinste unter den drei Potenzen $q'^{n'}, q'^{\beta'}, q'^{\gamma'}$ ist, also alle drei theilt, da endlich $q''^{\gamma''}$ die kleinste unter den drei Potenzen $q''^{\alpha''}, q''^{n''}, q''^{\gamma''}$ ist, also alle drei theilt, so müssen nothwendig K, K', K'' alle drei, also auch b, t, d alle drei, durch

$$q^\alpha q'^{\beta'} q''^{\gamma''}$$

theilbar sein.

Löset man die beiden Gleichungen für L' und L'' nach b' und t' auf, so erhält man

$$(1-\varrho^2)(\zeta_1-\varrho\zeta_2).b', \quad (1-\varrho^2)(\zeta_1-\varrho\zeta_2).t'$$

als lineäre Functionen von L', L''. Ebenso erhält man, wenn man die Gleichungen für L, L'', für L, L' nach b', t' auflöset,

$$(1-\varrho)(\zeta_1-\varrho^2\zeta_2).b', \quad (1-\varrho)(\zeta_1-\varrho^2\zeta_2).t'$$

als lineäre Functionen von L, L'' und

$$(\varrho^2-\varrho)(\zeta_1-\zeta_2).b', \quad (\varrho^2-\varrho)(\zeta_1-\zeta_2).t'$$

als lineäre Functionen von L, L'. Ich behaupte, dafs die drei Multiplicatoren

$$(1-\varrho^2)(\zeta_1-\varrho\zeta_2), \quad (1-\varrho)(\zeta_1-\varrho^2\zeta_2), \quad (\varrho^2-\varrho)(\zeta_1-\zeta_2)$$

zu a relative Primzahlen sind. In der That: da $1-\varrho$, $1-\varrho^2$, $\varrho^2-\varrho$ nicht in a aufgehen, so ist nur zu zeigen, dafs ζ_1 keiner der drei Zahlen ζ_2, $\varrho\zeta_2$, $\varrho^2\zeta_2$ nach einem Theiler von a congruent sein kann; wäre das letztere möglich, so müfste auch $\zeta_1^3 \equiv \zeta_2^3$ nach demselben Theiler sein: aber $\zeta_1^3 \equiv pp_1$, $\zeta_2^3 \equiv pp_2$ (mod. a), also müfste auch $pp_1 - pp_2$ einen gemeinschaftlichen Theiler mit a haben, gegen die Voraussetzung.

Da nun L' und L'' beide durch q^β, L und L'' beide durch $q'^{\gamma'}$, L und L' beide durch $q''^{\alpha''}$ theilbar sein sollen, so müssen b' und t' beide durch

$$q^\beta q'^{\gamma'} q''^{\alpha''}$$

theilbar sein. Aber das Product von

$$q^\alpha q'^{\beta'} q''^{\gamma''} \quad \text{und} \quad q^\beta q'^{\gamma'} q''^{\alpha''} \quad \text{ist} \quad = a,$$

und von der andern Seite ist $tt' = a$, also kann nur

$$t = q^\alpha q'^{\beta'} q''^{\gamma''}, \quad t' = q^\beta = q^\beta q'^{\gamma'} q''^{\alpha''}$$

gesetzt werden. ***Mithin haben nothwendig t und t' die beiden eben geschriebenen Werthe, b, d sind durch t, und b' ist durch t' theilbar.***

Die Congruenzen

$$K \equiv 0 \text{ (mod. } q^\alpha), \qquad L \equiv 0 \text{ (mod. } q^\alpha), \qquad L' \equiv 0 \text{ (mod. } q^\beta),$$

und ebenso die Congruenzen

$$K' \equiv 0 \text{ (mod. } q'^{\beta'}), \quad L' \equiv 0 \text{ (mod } q'^{\beta'}), \quad L'' \equiv 0 \text{ (mod. } q'^{\gamma'}), \text{ und}$$
$$K'' \equiv 0 \text{ (mod. } q''^{\gamma''}), \quad L'' \equiv 0 \text{ (mod. } q''^{\gamma''}), \quad L \equiv 0 \text{ (mod. } q''^{\alpha''})$$

sind durch diese Annahme schon befriedigt; es bleiben also für jede der drei Primzahlen noch drei Congruenzen zu lösen.

Zunächst ist jetzt b' so zu bestimmen, dafs

$$L'' \equiv 0 \text{ (mod. } q^n), \qquad L \equiv 0 \text{ (mod. } q'^{n'}), \qquad L' \equiv 0 \text{ (mod. } q''^{n''})$$

werde. Der ersten dieser drei letzteren Congruenzen genügt offenbar ein, und nur ein Werth von b', für welchen $0 \leqq b' < q^n$ ist; der zweiten genügt ein, und nur ein Werth von b', für welchen $0 \leqq b' < q'^{n'}$ ist; endlich genügt der dritten ein, und nur ein Werth von b', für welchen $0 \leqq b' < q''^{n''}$ ist: folglich genügt nach *Disq. arithm.* 33. allen dreien zugleich ein, und nur ein Werth von b', für welchen

$$0 \leqq b' < q^n q'^{n'} q''^{n''}, \quad \text{d. h.} \quad 0 \leqq b' < a \text{ ist.}$$

Für b', eben wie für t und t', stimmt also das Resultat mit der Behauptung vollkommen überein. Es bleibt noch die Betrachtung von b und d übrig, welche den drei folgenden Systemen von Congruenzen genügen müssen:

$$(25.) \quad \begin{cases} K' \equiv 0 \text{ (mod. } q^\beta), \\ K'' \equiv 0 \text{ (mod. } q^\gamma), \end{cases} \Bigg| \begin{matrix} K \equiv 0 \text{ (mod. } q'^{\alpha'}), \\ K' \equiv 0 \text{ (mod. } q'^{\gamma'}), \end{matrix} \Bigg| \begin{matrix} K \equiv 0 \text{ (mod. } q''^{\alpha''}), \\ K' \equiv 0 \text{ (mod. } q''^{\beta''}). \end{matrix}$$

Wir wollen besonders das erste dieser drei Systeme untersuchen; die beiden andern geben Veranlassung zu ganz ähnlichen Betrachtungen. Da $\gamma = n \geqq \beta$ ist, so wird die Congruenz $K'' \equiv 0$ auch nach dem Modul q^β erfüllt werden. Eliminirt man erst b, dann d aus den beiden Congruenzen $K' \equiv 0$ (mod. q^β), $K'' \equiv 0$ (mod. q^β), und bemerkt, dafs nach dieser Elimination der Multiplicator von b und d zu a relative Primzahl ist, so erhellet, dafs durch dieselben b, d nach dem Modul q^β vollständig bestimmt sind; man kann also d der Bedingung $0 \leqq d < q^\beta$ genügen lassen; ebenso kann man $b = b_0 + kq^\beta$ setzen, wo $0 \leqq b_0 < q^\beta$ und k eine unbestimmte ganze Zahl vorstellt; und d und b_0 werden vollkommen bestimmt sein. Es bleibt noch die Congruenz $K'' \equiv 0$ (mod. q^γ) zu erfüllen, d. h. die Congruenz

$$b_0 + kq^\beta + t(\varrho^2\zeta_1 + \varrho\zeta_2) + d(\zeta_1 + \zeta_2) \equiv 0 \pmod{q^\gamma = q^n}$$

oder

$$k \equiv -\frac{b_0 + t(\varrho^2\zeta_1 + \varrho\zeta_2) + d(\zeta_1 + \zeta_2)}{q^\beta} \pmod{q^{n-\beta} = q^\alpha},$$

welche, da der Bruch zur Rechten dem Vorigen zufolge einer ganzen Zahl gleich ist, einen vollkommen bestimmten Werth für k liefert, für welchen $0 \leqq k < q^\alpha$ ist. Dadurch aber ist auch b vollkommen und der Bedingung $0 \leqq b < q^n$ genügend bestimmt.

Durch das erste der drei Systeme (25.) sind also b, d vollkommen nach den Moduln resp. q^n, q^β bestimmt; ebenso sind durch die beiden andern Systeme (25.) b, d respective nach den Moduln $q'^{\alpha'} = q'^{n'}$, $q'^{\gamma'}$; $q''^{\beta''} = q''^{n''}$, $q''^{\alpha''}$ vollkommen bestimmt; da also b und d allen drei Systemen zugleich genügen sollen, so ist

b vollkommen nach den Moduln q^n, $q'^{n'}$, $q''^{n''}$ bestimmt, also auch nach ihrem Producte a;

d ist vollkommen nach den Moduln q^β, $q'^{\gamma'}$, $q''^{\alpha''}$ bestimmt, also auch nach ihrem Producte $q^\beta q'^{\gamma'} q''^{\alpha''} = t'$:

folglich giebt es nur einen Werth von b und nur einen Werth von d, für welche

$$0 \leqq b < a, \quad 0 \leqq d < t'$$

ist, und welche den sechs Congruenzen (25.) genügen.

Dasselbe Resultat erhält man, wie grofs man auch die Anzahl der verschiedenen Primfactoren von a, und welche Combination (E.) der Exponenten man auch nehmen mag. Um uns verständlicher zu machen, nennen wir den kleinsten Factor die kleinste von dreien Potenzen, wie q^α, q^β, q^γ; ebenso den

gröfsten und mittleren Factor die gröfste und mittlere von solchen drei Potenzen; und analog, wenn alle Buchstaben beliebig oft accentuirt sind. Wie grofs nun auch die Anzahl der Primfactoren von a sein mag, und welche Combinationen der Exponenten man auch bilden mag: immer wird sich durch dieselben Betrachtungen wie oben zeigen lassen, *dafs t gleich sein mufs dem Producte aller kleinsten, t' gleich dem Producte aller mittleren Factoren, und dafs b, d durch t, und b' durch t' theilbar sein müssen.* Durch diese Annahmen wird schon der einen Hälfte aller zu erfüllenden Congruenzen genügt, während von der andern Hälfte ein Drittheil die Zahl b' nach allen gröfsten Factoren als Moduln, also auch nach ihrem Producte a vollständig bestimmt, und die andern zwei Drittheile die Zahlen b, d nach allen resp. gröfsten, mittleren Factoren, als Moduln, also auch nach a resp. t' vollständig bestimmen. Jeder Combination entspricht also ein vollständig bestimmtes t und t', und ein, aber auch nur ein System von Werthen für b, d und b', für welche

$$0 \leqq b < a, \quad 0 \leqq d < t', \quad 0 \leqq b' < a \text{ ist.}$$

Alle die so gefundenen Systeme genügen der Bedingung (B.), denn es ist $cd' - c'd = tt' - 0.d = tt' = a$.

Könnte man also noch zeigen, dafs für alle diese Systeme die 10 Coëfficienten des entwickelten Products (18.) zwar durch a^2, aber aufserdem durch keine andere Zahl theilbar sind, so würde unsere Behauptung vollständig erwiesen sein. Welches auch der gröfste gemeinschaftliche Theiler h dieser 10 Coëfficienten sein mag, immer mufs er ein Theiler von a^3 sein; denn a^3 ist der erste der 10 Coëfficienten. Aber das Product der drei Factoren in (20.) ist in Bezug auf alle zehn Coëfficienten dem Producte (18.) nach dem Modul a^3 congruent, folglich ist auch h gröfster gemeinschaftlicher Theiler der Coëfficienten des Products (20.). Ginge nun irgend ein Primfactor von a, z. B. q, von einer höhern Potenz in h auf, als in welcher er in a^2 enthalten ist, so müfste sich diese Potenz von q nach II. dergestalt auf die drei Linearfactoren (20.) vertheilen, dafs der erste, zweite, dritte seine drei Coëfficienten resp. durch q^α, q^β, q^γ theilbar haben müfste, während $\alpha+\beta+\gamma > 2n$ wäre. Aus dieser Annahme schliefst man, ganz wie oben in V., dafs die Summe der beiden kleinsten von den drei Zahlen α, β, γ, z. B. $\beta+\gamma \leqq n$ sein mufs, also auch $\alpha+\beta+\gamma \leqq n+\alpha$: aber jetzt ist nicht wie oben $2n = \alpha+\beta+\gamma$, sondern $2n < \alpha+\beta+\gamma$, also folgt $2n < n+\alpha$, $n < \alpha$; aber auch $n \geqq \alpha$, weil a durch q^α theilbar sein soll, folglich ist zu gleicher Zeit $n < \alpha$ und $n \geqq \alpha$, was sich widerspricht; also ist nothwendig $h = a^2$; denn

dafs die höchste in h enthaltene Potenz irgend eines Primfactors q von a auch nicht $< q^{2n}$ sein kann, erhellet schon aus der obigen Bestimmung der Werthe von b, d, b', t, t'.

VII. Da jeder Combination aus nicht-negativen ganzen Zahlen

$$(E.) \quad \begin{cases} \alpha, & \beta, & \gamma, \\ \alpha', & \beta', & \gamma', \\ \alpha'', & \beta'', & \gamma'', \\ \alpha''', & \beta''', & \gamma''', \\ \ldots & \ldots & \ldots, \end{cases}$$

wo in der ersten Horizontalreihe ein Element und die Summe der beiden andern $= n$, in der zweiten Horizontalreihe ein Element und die Summe der beiden andern $= n'$ ist u. s. w., eine und nur eine reducirte Form entspricht, und da alle diese reducirten Formen verschieden sind (denn für jede gegebene reducirte Form sind die drei Factoren des Products (20.) vollkommen bestimmt, und da sämmtliche Coëfficienten dieses Products durch a^2 und nur durch a^2 theilbar sind, so entspricht jeder reducirten Form nur eine vollkommen bestimmte Vertheilung der Factoren von a^2 auf die drei Factoren des Products (20.) also auch eine und nur eine vollkommen bestimmte Combination (*E.*)): so ist die *Anzahl aller reducirten Formen gleich der Anzahl der möglichen Combinationen* (*E*). Man erhält die Anzahl dieser letzteren offenbar, wenn man einzeln die Anzahl der Combinationen α, β, γ, die Anzahl der Combinationen α', β', γ', die Anzahl der Combinationen $\alpha'', \beta'', \gamma''$, u. s. w. bestimmt und das Product aller dieser einzelnen Combinationszahlen bildet. Alle Combinationen α, β, γ sind in dem folgenden Schema enthalten:

$\alpha,$	$\beta,$	γ	$\alpha,$	$\beta,$	γ	$\alpha,$	$\beta,$	γ
$n,$	$0,$	n	$n,$	$n,$	0	$0,$	$n,$	n
$n,$	$1,$	$n-1$	$n-1,$	$n,$	1	$1,$	$n-1,$	n
$n,$	$2,$	$n-2$	$n-2,$	$n,$	2	$2,$	$n-2,$	n
$n,$	$3,$	$n-3$	$n-3,$	$n,$	3	$3,$	$n-3,$	n
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
$n,$	$n-2,$	2	$2,$	$n,$	$n-2$	$n-2,$	$2,$	n
$n,$	$n-1,$	1	$1,$	$n,$	$n-1$	$n-1,$	$1,$	$n;$

ihre Anzahl ist folglich $= 3n$; ebenso ist $3n'$ die Anzahl der Combinationen α', β', γ', $3n''$ die Anzahl der Combinationen $\alpha'', \beta'', \gamma''$, u. s. w.; mithin ist die Anzahl aller Combinationen (*E.*)

$$= 3n.3n'.3n''.3n''' \ldots:$$

ebenso grofs ist also auch die Anzahl der reducirten Formen.

Folgendes ergiebt sich demnach als Resultat der Untersuchung:

„Damit es reducirte Formen mit dem ersten Coëfficienten a gebe, welcher relative Primzahl zu $2(pp_1 - pp_2)$ vorausgesetzt wird, ist es nöthig und hinreichend, dafs jeder reelle Primfactor von a cubischer Rest zu p sei. Wenn diese Bedingung erfüllt wird, so lassen sich alle reducirten Formen nach Anweisung von IV., V. und VI. finden; und setzt man

$$a = q_1^{n_1} q_2^{n_2} q_3^{n_3} \ldots q_\mu^{n_\mu};$$

so wird die Anzahl der zu a gehörigen reducirten Formen durch die Formel

$$3^\mu . n_1 . n_2 . n_3 \ldots n_\mu$$

ausgedrückt, also durch das Product aller Exponenten der verschiedenen Primfactoren von a, multiplicirt mit einer Potenz von 3, deren Exponent gleich ist der Anzahl dieser Primfactoren.“

Man bemerke wohl, dafs das Resultat seine Gültigkeit in dem Falle $a = 1$ nicht verliert; in diesem speciellen Falle sind gar keine Primfactoren $q > 1$ vorhanden, also giebt unsere Formel $3^0 = 1$; und in der That existirt nur eine reducirte Form mit dem ersten Coëfficienten 1, nämlich die Grundform Φ, für welche $b = 0$, $c = 1$, $d = 0$, $b' = 0$, $c' = 0$, $d' = 1$, $t = t' = 1$ ist.

Wir gehen zu der Transformation der associirten Formen über.

§. 8.

Theorie der Transformation der associirten Formen.

I. „Wenn zwei lineäre Systeme mit 3 Variabeln, S und T, deren Determinante wir $= 1$ voraussetzen, durch ihre Zusammensetzung das System S' hervorbringen, so behaupte ich Folgendes: 1) Sind die Coëfficienten beider Systeme S und T ganze Zahlen, so sind die Coëfficienten des Systems S' ganze Zahlen. 2) Sind die Coëfficienten eines der zusammensetzenden Systeme und die des zusammengesetzten Systems ganze Zahlen, so findet dies auch für das zweite zusammensetzende System Statt. 3) Sind die Coëfficienten des einen zusammensetzenden Systems ganze Zahlen und die des andern Brüche mit dem Nenner m, welcher wenigstens in einem Coëfficienten keine weitere Reduction zuläfst, so können auch die Coëfficienten von S' nicht sämmtlich ganze Zahlen sein, sondern einige oder alle werden den Nenner m haben, aber auch keinen andern Nenner, und wenigstens ein Coëfficient des Systems S' wird ein irreducibler Bruch sein. 4) Wenn S und S' gegebene Systeme

mit ganzen Coëfficienten sind, so läfst sich immer ein, und nur ein System T mit ganzen Coëfficienten aufstellen, welches mit S zusammengesetzt S' hervorbringt; und sind T und S' mit ganzen Coëfficienten gegeben, so läfst sich immer ein, und nur ein System S aufstellen, welches mit T zusammengesetzt S' hervorbringt; oder, mit andern Worten: in der symbolischen Gleichung zwischen Systemen mit ganzen Coëfficienten

$$S \times T = S'$$

ist jedes der drei Systeme durch die beiden andern vollständig bestimmt."

Alle diese Behauptungen folgen mit Leichtigkeit aus dem Umstande, dafs die Coëfficienten eines zusammengesetzten Systems lineäre Functionen sind, sowohl in Beziehung auf die Coëfficienten des einen, als auf die des andern der beiden zusammensetzenden Systeme. Hieraus ergiebt sich die erste Behauptung unmittelbar. Was die zweite Behauptung betrifft, so bemerke man, dafs die Determinante des Systems S, so wie die des Systems T, der Einheit gleich ist; dafs folglich die umgekehrten Systeme von S, T, welche wir resp. durch $\frac{1}{S}$, $\frac{1}{T}$ bezeichnen, mit resp. S, T zugleich ganze Coëfficienten haben. Da nun offenbar $S = S' \times \frac{1}{T}$, $T = \frac{1}{S} \times S'$ ist, so findet sich die zweite Behauptung auf die erste zurückgeführt. Da ferner aus der lineären Beschaffenheit der Coëfficienten von S' folgt, dafs, unter Voraussetzung ganzer Coëfficienten für eines der beiden Systeme S oder T, der Generalnenner der Coëfficienten des andern durch den Generalnenner derer von S' theilbar sein mufs, und da umgekehrt, wegen $S = S' \times \frac{1}{T}$, oder wegen $T = \frac{1}{S} \times S'$, auf ähnliche Art folgt, dafs der erste Generalnenner ein Theiler des zweiten sein mufs, so theilen diese beiden Generalnenner sich gegenseitig, und sind folglich einander gleich; und somit ist auch die dritte Behauptung erwiesen. Die vierte Behauptung ist ebenfalls leicht zu beweisen. Wenn die beiden Systeme S und T gegeben sind, so ist dadurch S' vollkommen bestimmt; und haben die beiden ersteren ganze Coëfficienten, so wird dies nach 1) auch für das letztere der Fall sein. Es sei T ein noch unbekanntes System, welches der Gleichung $S \times T = S'$ genügt: da die beiden Systeme zur Linken und zur Rechten dieser Gleichung identisch sein sollen, so wird diese Identität nicht aufhören, wenn man das System $\frac{1}{S}$ mit beiden zusammensetzt; wodurch man $T = \frac{1}{S} \times S'$ erhält; so dafs also für T dieses, und nur dieses vollkommen bestimmte System genommen werden mufs. Ebenso erhält man, wenn T und S'

gegeben sind, durch Zusammensetzung beider Seiten der Gleichung $S \times T = S'$ mit dem System $\frac{1}{T}$, für S das vollkommen bestimmte System

$$S = S' \times \frac{1}{T}.$$

Alles dieses gilt auch für lineare Systeme mit n Variabeln, deren Determinante $= 1$ ist. Man kann hierauf beiläufig einen Algorithmus der Rechnung mit linearen Systemen gründen; welcher darin besteht, dafs man auf symbolische Gleichungen zwischen linearen Systemen die gewöhnlichen Regeln für die Operationen des Multiplicirens, Dividirens und Potenziirens anwendet; was immer richtige symbolische Gleichungen erhält und wobei man nur die einzige Rücksicht zu nehmen hat, dafs die Ordnung der Factoren, d. h. die Ordnung der zusammensetzenden Systeme, *nicht* verändert werden darf.

Es seien F, G, F' drei aequivalente associirte Formen; S sei eine bestimmte Transformation, durch welche F in G übergeht, und T stelle alle möglichen Transformationen vor, durch welche G in F' übergeht: dann behaupte ich, dafs S', welches durch die symbolische Gleichung $S' = S \times T$ gegeben ist, alle möglichen Transformationen von F in F' vorstellen wird. Denn einerseits geht F in G durch S, G in F' durch T, also F in F' durch die zusammengesetzte Substitution S' über; und andrerseits entspricht jedem S' ein vollkommen bestimmtes T, welches der obigen Gleichung genügt und durch welches G in F' übergeht; man zieht aus obiger Gleichung für T das vollkommen bestimmte System $T = \frac{1}{S} \times S'$, und durch diese Substitution geht in der That G in F' über; denn durch die Substitution $\frac{1}{S}$ geht G in F und durch die Substitution S' geht nach der Annahme F in F' über, also geht durch die zusammengesetzte Substitution $\frac{1}{S} \times S'$ die Form G in F' über. Umgekehrt: wenn S eine bestimmte Substitution von F in G, und S' nach der Reihe alle möglichen Substitutionen von F in F' vorstellt, so liefert die Gleichung $S \times T = S'$ für T alle Substitutionen, durch welche G in F' übergeht; denn diese Gleichung liefert für jedes T ein ganz bestimmtes S' und für jedes S' ein ganz bestimmtes T, welches, wie schon bewiesen, G in F transformirt. Setzt man demnach statt S' alle möglichen Substitutionen, welche F in F' transformiren, so liefert die Gleichung für jede derselben eine, und nur eine Substitution T, welche G in F' transformirt; es kann auch keine andere Transformation von G in F' geben, welche sich nicht auf diese Art vermöge der Gleichung aus einer Transformation von F in F' ableiten liefse; denn

es sei, wenn es möglich ist, T eine von diesen andern Transformationen; da G durch T in F' und F in G durch S übergeht, so geht F in F' durch $S \times T$ über; also ist doch wieder $S \times T = S'$ eine von den Transformationen, durch welche F in F' übergeht. Ganz auf dieselbe Weise beweiset man folgende Sätze. Wenn in der symbolischen Gleichung $S \times T = S'$ durch S alle möglichen Transformationen von F in G und durch T eine bestimmte Transformation von G in F' vorgestellt werden, so giebt S' alle möglichen Transformationen von F in F'; und umgekehrt: bezeichnet S' alle möglichen Transformationen von F in F', während T dieselbe Bedeutung behält, so giebt S alle möglichen Transformationen von F in G. Wenn endlich in der oft geschriebenen Gleichung S alle möglichen Transformationen von F in G und S' eine bestimmte Transformation von F in F' bezeichnet, so giebt T alle möglichen Transformationen von G in F'; und bezeichnet T alle möglichen Transformationen von G in F' und S' eine bestimmte Transformation von F in F', so giebt S alle möglichen Transformationen von F in G. Alle diese Resultate lassen sich kurz wie folgt aussprechen.

„Wenn in der symbolischen Gleichung

$$S \times T = S'$$

irgend einer der drei Buchstaben alle seine Werthe durchläuft, während ein zweiter constant bleibt, so durchläuft der dritte ebenfalls alle seine Werthe."

Nimmt man in den eben gewonnenen Resultaten irgend zwei von den drei Formen als identisch an, d. h. setzt man entweder $F = G$, oder $G = F'$, oder $F = F'$, so erhält man die folgenden. Alle Substitutionen einer Form F in eine Form G ergeben sich, wenn man irgend eine bestimmte von denselben mit allen Substitutionen von G *in sich selbst* zusammensetzt, oder auch, wenn man mit ersterer alle Substitutionen von F in sich selbst zusammensetzt; und umgekehrt: bezeichnet S alle Substitutionen von F in G und S_0 eine bestimmte von ihnen, so findet man alle Substitutionen von F in sich selbst, wenn man zu jeder Substitution S eine zugehörige sucht, die, mit S_0 zusammengesetzt, S hervorbringt, und alle Substitutionen von G in sich selbst, wenn man zu jeder S eine solche sucht, mit welcher S_0 zusammengesetzt S hervorbringt.

Allgemeiner ist folgende Betrachtung. Es sind fünf aequivalente associirte Formen

$$F,\ G,\ H,\ I,\ K$$

vorgelegt; man kennt eine Transformation $\mathfrak{A}$ von F in G, eine $\mathfrak{B}$ von F

in H, eine $\mathfrak{C}$ von F in I, eine $\mathfrak{D}$ von F in K, aufserdem aber noch alle möglichen Transformationen S von I in K: es sollen aus diesen Daten alle Substitutionen von G in H gefunden werden.

Es geht über:	durch die Substitution
F in G	$\mathfrak{A}$,
also G in F	$\frac{1}{\mathfrak{A}}$;
F in I	$\mathfrak{C}$,
also G in I	$\frac{1}{\mathfrak{A}}\times\mathfrak{C}$;
I in K	S,
also G in K	$\frac{1}{\mathfrak{A}}\times\mathfrak{C}\times S$;
K in F	$\frac{1}{\mathfrak{D}}$,
also G in F	$\frac{1}{\mathfrak{A}}\times\mathfrak{C}\times S\times\frac{1}{\mathfrak{D}}$;
F in H	$\mathfrak{B}$,
also G in H	$\frac{1}{\mathfrak{A}}\times\mathfrak{C}\times S\times\frac{1}{\mathfrak{D}}\times\mathfrak{B} = T$.

Diese letztere Formel liefert also Transformationen von G in H, und wenn man denselben Weg rückwärts einschlägt, so zeigt sich, dafs jedem T ein ganz bestimmtes S entspricht und dafs also T *alle* Transformationen von G in H liefert.

Man sieht demnach, dafs alle Probleme über Transformationen von Formen auf die Transformation irgend zweier beliebigen Formen aus derselben Classe in einander, oder, da diese beiden letzteren identisch angenommen werden können, auf die Transformation irgend einer beliebigen Form derselben Classe, in sich selbst zurückgeführt werden können.

II. Aufgabe. „Alle Transformationen (mit ganzen Coëfficienten) zu finden, durch welche eine associirte Form in sich selbst übergeht."

Es sei F die gegebene associirte Form, a ihr erster Coëfficient,

$$a^2F = (au+\lambda v+\lambda' w)(au+\mu v+\mu' w)(au+\nu v+\nu' w) = \varphi(u,v,w)\psi(u,v,w)\chi(u,v,w),$$

$$\lambda = b+e\eta+f\vartheta, \qquad \lambda' = b'+e'\eta+f'\vartheta,$$
$$\mu = b+e\varrho\eta+f\varrho^2\vartheta, \qquad \mu' = b'+e'\varrho\eta+f'\varrho^2\vartheta,$$
$$\nu = b+e\varrho^2\eta+f\varrho\vartheta, \qquad \nu' = b'+e'\varrho^2\eta+f'\varrho\vartheta,$$

$$e = c + d\varrho, \qquad f = c + d\varrho^2,$$
$$e' = c' + d'\varrho, \qquad f' = c' + d'\varrho^2,$$
$$cd' - c'd = a; \qquad \eta = \sqrt[3]{(pp_1)}, \qquad \vartheta = \sqrt[3]{(pp_2)}.$$

Wenn die Form F durch die Substitution

$$(1.) \qquad \begin{Bmatrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{Bmatrix}$$

in sich selbst übergeht, so bleibt auch a^2F durch diese Substitution unverändert; und umgekehrt. Wir haben also alle Substitutionen (1.) zu suchen, durch welche a^2F unverändert bleibt. Durch die Substitution (1.) gehen die drei Linearfactoren von a^2F in

$$(Iu + Kv + Lw), \qquad (I'u + K'v + L'w), \qquad (I''u + K''v + L''w)$$

über, wo man

$$I = a\alpha + \lambda\beta + \lambda'\gamma = \varphi(\alpha, \beta, \gamma), \quad K = a\alpha' + \lambda\beta' + \lambda'\gamma' = \varphi(\alpha', \beta', \gamma'), \quad L = a\alpha'' + \lambda\beta'' + \lambda'\gamma'' = \varphi(\alpha'', \beta'', \gamma''),$$
$$I' = a\alpha + \mu\beta + \mu'\gamma = \psi(\alpha, \beta, \gamma), \quad K' = a\alpha' + \mu\beta' + \mu'\gamma' = \psi(\alpha', \beta', \gamma'), \quad L' = a\alpha'' + \mu\beta'' + \mu'\gamma'' = \psi(\alpha'', \beta'', \gamma''),$$
$$I'' = a\alpha + \nu\beta + \nu'\gamma = \chi(\alpha, \beta, \gamma), \quad K'' = a\alpha' + \nu\beta' + \nu'\gamma' = \chi(\alpha', \beta', \gamma'), \quad L'' = a\alpha'' + \nu\beta'' + \nu'\gamma'' = \chi(\alpha'', \beta'', \gamma'')$$

hat. Das Product dieser drei Factoren mufs also dem Producte der drei ursprünglichen Factoren von a^2F identisch gleich werden. Da wir nur alle Substitutionen suchen, durch welche F *in sich selbst*, und *nicht* zugleich alle diejenigen, durch welche F in eine ihrer *correspondirenden Formen* übergeht, so haben wir nach dem in §. 5. III. Bemerkten nur folgende Annahmen zu machen: erstlich

$$(2.) \qquad \frac{I}{a} \cdot \frac{I'}{a} \cdot \frac{I''}{a} = 1,$$

und zweitens

$$(3.) \qquad \frac{I}{a} = \frac{K}{\lambda} = \frac{L}{\lambda'}; \qquad \frac{I'}{a} = \frac{K'}{\mu} = \frac{L'}{\mu'}; \qquad \frac{I''}{a} = \frac{K''}{\nu} = \frac{L''}{\nu'};$$

wo offenbar alle Nenner von Null verschieden sind; und diese Annahmen sind erforderlich und hinreichend für die Identität unserer beiden Producte. Man sieht übrigens, dafs das erste System von Gleichungen in (3.) das zweite und dritte als correspondirende Relationen implicite enthält, so dafs also nur jenes zu berücksichtigen ist. Die Aufgabe besteht jetzt darin, alle ganzen Werthe der Transformationscoëfficienten in (1.) zu finden, welche den Gleichungen (2.) und (3.) genügen und welche die Determinante des Systems (1.) der Einheit gleich machen.

Setzt man, was offenbar erlaubt ist,

$$\frac{I}{a} = U + Y\eta + Z\vartheta = A,$$
$$\frac{I'}{a} = U + Y\varrho\eta + Z\varrho^2\vartheta = B,$$
$$\frac{I''}{a} = U + Y\varrho^2\eta + Z\varrho\vartheta = C,$$

wo $Y = V + W\varrho$, $Z = V + W\varrho^2$ und U, V, W im Allgemeinen *rationale* und reelle Zahlen vorstellen, so geht die Gleichung (2.) in

$$(4.)\quad U^3 + pp_1 Y^3 + pp_2 Z^3 - 3pUYZ = 1 \text{ über,}$$

und das erste System von Gleichungen in (3.) liefert

$$(5.)\quad I = aA,\quad K = \lambda A,\quad L = \lambda' A.$$

Vergleicht man in jeder dieser letzteren drei Gleichungen einzeln die reellen Theile und die Coëfficienten von η und von ϑ, so erhält man die folgenden neun:

$$\left.\begin{array}{ll}(6.) & a\alpha + b\beta + b'\gamma = aU,\\ (7.) & e\beta + e'\gamma = aY,\\ (8.) & f\beta + f'\gamma = aZ,\end{array}\right\}\ (\mathfrak{A}.)$$

$$\left.\begin{array}{ll}(9.) & a\alpha' + b\beta' + b'\gamma' = bU + pfY + peZ,\\ (10.) & e\beta' + e'\gamma' = eU + bY + p_2 fZ,\\ (11.) & f\beta' + f'\gamma' = fU + p_1 eY + bZ,\end{array}\right\}\ (\mathfrak{B}.)$$

$$\left.\begin{array}{ll}(12.) & a\alpha'' + b\beta'' + b'\gamma'' = b'U + pf'Y + pe'Z,\\ (13.) & e\beta'' + e'\gamma'' = e'U + b'Y + p_2 f'Z,\\ (14.) & f\beta'' + f'\gamma'' = f'U + p_1 e'Y + b'Z.\end{array}\right\}\ (\mathfrak{C}.)$$

Diese neun Gleichungen dienen zur Bestimmung der 9 Transformationscoëfficienten; sie ordnen sich in drei Systeme zu je dreien, indem (6.), (7.), (8.) blofs α, β, γ; (9.), (10.), (11.) blofs α', β', γ', und (12.), (13.), (14.) blofs α'', β'', γ'' enthalten. Es sind also jetzt alle rationalen Werthe von U, V, W zu bestimmen, welche der Gleichung (4.) genügen und welche, in die Gleichungen (6.) bis (14.) gesetzt, bewirken, dafs diese letzteren nach α, β, γ, α', β', γ', α'', β'', γ'' aufgelöset 1) *ganze* Werthe für diese Transformationscoëfficienten ergeben, und 2) solche Werthe, für welche die Determinante des Systems (1.) der Einheit gleich wird. Um zuerst diese zweite Bedingung zu erledigen, seien U, V, W beliebige bestimmte rationale Werthe, die der Gleichung (4.) genügen, und die Systeme ($\mathfrak{A}$.), ($\mathfrak{B}$.), ($\mathfrak{C}$.) seien nach den Transformationscoëfficienten aufgelöset, für welche sie vollkommen bestimmte Werthe liefern, indem die Determinante dieser drei Systeme $= a(ef' - e'f) = a(\varrho^2 - \varrho)(cd' - c'd) = (\varrho^2 - \varrho)a^2$, also von Null verschieden ist: ich behaupte,

dafs die so gefundenen Werthe die Determinante von (1.) immer $=1$ machen werden. Es sei für einen Augenblick diese Determinante durch $\varDelta$ vorgestellt. Das System

$$\left\{\begin{matrix} I, & K, & L \\ I', & K', & L' \\ I'', & K'', & L'' \end{matrix}\right\} = S,$$

dessen Determinante wir durch $\varDelta'$ bezeichnen, ist offenbar zusammengesetzt aus dem System

$$\left\{\begin{matrix} a, & \lambda, & \lambda' \\ a, & \mu, & \mu' \\ a, & \nu, & \nu' \end{matrix}\right\} = T,$$

dessen Determinante $=\varDelta''$ sei, und aus (1.); also hat man $\varDelta' = \varDelta.\varDelta''$. Dividirt man die drei Horizontalreihen des Systems S resp. durch $\frac{I}{a}$, $\frac{I'}{a}$, $\frac{I''}{a}$, so ergiebt sich das System

$$\left\{\begin{matrix} a, & \frac{aK}{I}, & \frac{aL}{I} \\ a, & \frac{aK'}{I'}, & \frac{aL'}{I'} \\ a, & \frac{aK''}{I''}, & \frac{aL''}{I''} \end{matrix}\right\} = S',$$

dessen Determinante offenbar gleich $\frac{a}{I}.\frac{a}{I'}.\frac{a}{I''}.\varDelta' = \frac{a}{I}.\frac{a}{I'}.\frac{a}{I''}.\varDelta.\varDelta''$ sein wird. Da nun die Gleichungen (6.) bis (14.) und die Gleichung (4.) als erfüllt angenommen werden, so werden auch die Gleichungen (3.) und die Gleichung (2.) erfüllt sein; die Gleichungen (3.) zeigen, dafs die beiden Systeme S' und T vollkommen identisch sind und dafs also auch ihre Determinanten identisch sind; folglich hat man

$$\varDelta'' = \frac{a}{I}.\frac{a}{I'}.\frac{a}{I''}.\varDelta.\varDelta'',$$

mithin, wegen (2.), $\varDelta = 1$; was zu beweisen war. Da sich also die zweite der oben gedachten Bedingungen immer erfüllt findet, so ist nur noch die erste zu befriedigen. Zu dem Ende stellen wir die beiden folgenden Behauptungen auf:

1) *Damit die Gleichungen* (6.) *bis* (14.) *ganze Werthe für alle neun Transformationscoëfficienten liefern, ist erforderlich, dafs U, V, W selbst ganze Zahlen sind,* und

2) *Wenn U, V, W irgend welche ganze Zahlen vorstellen, die der Gleichung (4.) genügen, so liefern die Gleichungen (6.) bis (14.) immer ganze Werthe für alle 9 Transformationscoëfficienten.*

Wir sind für den Augenblick noch nicht im Stande, diese beiden Behauptungen vollständig zu beweisen, deren Richtigkeit sich erst weiter unten mit Evidenz ergeben wird, sondern müssen uns für jetzt mit folgenden Bemerkungen begnügen. Aus den Gleichungen (𝔄.) folgt, dafs ganzen Werthen der Transformationscoëfficienten immer ganze Werthe von aU, aV, aW entsprechen und dafs man sich folglich umgekehrt, um ganze Werthe der ersteren zu erhalten, keiner andern Werthe von U, V, W bedienen darf, als solcher, die in den Formeln

$$(15.)\quad U = \frac{U'}{a},\quad V = \frac{V'}{a},\quad W = \frac{W'}{a}$$

enthalten sind, wo U', V', W' ganze Zahlen sind. Löset man die Gleichungen (6.) bis (14.) nach α, β, γ; α', β', γ'; α'', β'', γ'' auf, so zeigt sich, selbst ohne diese Operation wirklich auszuführen, dafs in die Formeln für diese Unbekannten keine andern Nenner eingehen können, als erstlich der schon in U, V, W enthaltene Nenner a, und zweitens die Determinante der Systeme (𝔄.), (𝔅.), (ℭ.), deren Werth wie schon bemerkt $= a(ef'-e'f) = (\varrho^2-\varrho)a^2$ ist; und da $\varrho^2-\varrho$ offenbar weggeschafft werden kann (am besten sieht man dies letztere ein, wenn man die Gleichungen (6.) bis (14.) so zerfället, dafs sie nur reelle Gröfsen enthalten), so sieht man, dafs die so erhaltenen Werthe von α, β u. s. w. höchstens a^3 oder einen Theiler von a^3 zum Generalnenner haben können.

Aus diesem Allen läfst sich wenigstens Folgendes schliefsen. „Es giebt keine andern Transformationen von F in sich selbst, als solche, die in den Gleichungen (5.), d. h. in den die neun Gleichungen (6.) bis (14.) implicite vorstellenden Gleichungen

$$(16.)\quad \varphi(\alpha,\beta,\gamma) = u.A;\quad \varphi(\alpha',\beta',\gamma') = \lambda.A;\quad \varphi(\alpha'',\beta'',\gamma'') = \lambda'.A$$

enthalten sind, wo

$$A = U+(V+W\varrho)\eta+(V+W\varrho^2)\vartheta \text{ ist,}$$

U, V, W alle rationalen Zahlen mit dem Nenner a oder einem Theiler von a bezeichnen, die der Gleichung (4.) genügen. Und alle Systeme von α, β u. s. w., welche sich zu den verschiedenen Systemen U, V, W durch Auflösung von (16.) ergeben, und von denen nur die *ganzen* als Lösungen des Problems zugelassen werden dürfen, können, wenn auch Brüche, doch keinen andern Generalnenner haben, als a^3, oder einen Theiler von a^3."

Wir wiederholen nochmals, um der vollkommenen Strenge nichts zu vergeben und um jedes Mifsverständnifs zu verhüten, dafs es nach dem Bisherigen möglich sein könnte, dafs vielleicht die Formel (16.) für alle Werthe von U, V, W, deren Generalnenner ein Theiler von a ist, kein einziges ganzes Transformationssystem (1.) lieferte; indessen wissen wir bestimmt, dafs es keine andern Transformationen von F in sich selbst geben kann, die nicht durch (16.) geliefert würden, und dafs die gebrochenen Werthe von α, β u. s. w., welche (16.) giebt, keinen andern Generalnenner haben können, als einen solchen, der in a^3 aufgeht; und alle diese Resultate gelten für jede zweite, von F verschiedene Form, wenn man an die Stelle von a den ersten Coëfficienten dieser neuen Form und an die Stelle von φ den ersten Linearfactor dieser neuen Form setzt.

III. „Es sind zwei aequivalente associirte Formen F_1 und F, so wie eine Transformation (natürlich mit ganzen Coëfficienten)

$$(17.)\quad \begin{Bmatrix} \alpha_1, & \alpha'_1, & \alpha''_1 \\ \beta_1, & \beta'_1, & \beta''_1 \\ \gamma_1, & \gamma'_1, & \gamma''_1 \end{Bmatrix}$$

von F_1 in F gegeben: man soll alle Transformationen finden, welche dieselbe Wirkung hervorbringen."

Es sei a^2F auf dieselbe Form gebracht, wie oben in II.; es sei a_1 der erste Coëfficient von F_1, und

$$\begin{aligned} a_1^2 F_1 &= (a_1 u_1 + \lambda_1 v_1 + \lambda'_1 w_1)(a_1 u_1 + \mu_1 v_1 + \mu'_1 w_1)(a_1 u_1 + \nu_1 v_1 + \nu'_1 w_1) \\ &= \varphi_1(u_1, v_1, w_1)\,\psi_1(u_1, v_1, w_1)\,\chi_1(u_1, v_1, w_1), \end{aligned}$$

wo λ_1, λ'_1 u. s. w. eben so aus b_1, c_1 u. s. w. zusammengesetzt sein sollen, wie oben λ, λ' u. s. w. aus b, c u. s. w. Man erhält nach I. dieses Paragraphen alle gesuchten Substitutionen, und jede nur einmal, wenn man das System (17.) mit allen Substitutionen von F in sich selbst zusammensetzt, also mit allen Systemen (1.), welche sich aus den Formeln (16.) als ganze Systeme (d. h. als Systeme mit ganzen Coëfficienten) ergeben; ferner erhellet aus I., dafs, wenn man bei dieser Zusammensetzung den Formeln (16.) nicht blofs die ganzen, sondern alle Systeme (1.) entlehnen wollte, der Generalnenner des zusammengesetzten Systems (d. h. der Generalnenner seiner Coëfficienten) gleich sein würde dem Generalnenner des angewandten Systems (1.), also ebenfalls, wie dieser, ein Theiler von a^3. Da nach der Voraussetzung F_1 in F durch (17.) übergeht, so kann man, wie aus dem Beweise des Lehrsatzes 5. in §. 5. hervorgeht, a, λ, λ', wie folgt ausdrücken:

$$a = \frac{\varphi_1(\alpha_1,\beta_1,\gamma_1)\psi_1(\alpha_1,\beta_1,\gamma_1)\chi_1(\alpha_1,\beta_1,\gamma_1)}{a_1^2},$$
$$\lambda = \frac{\varphi_1(\alpha'_1,\beta'_1,\gamma'_1)\psi_1(\alpha_1,\beta_1,\gamma_1)\chi_1(\alpha_1,\beta_1,\gamma_1)}{a_1^2},$$
$$\lambda' = \frac{\varphi_1(\alpha''_1,\beta''_1,\gamma''_1)\psi_1(\alpha_1,\beta_1,\gamma_1)\chi_1(\alpha_1,\beta_1,\gamma_1)}{a_1^2}.$$

Substituirt man diese Werthe in den Formeln (16.), so ergiebt sich

$$(18.)\quad\begin{cases}\varphi_1(\alpha_1,\beta_1,\gamma_1)\alpha\;+\varphi_1(\alpha'_1+\beta'_1+\gamma'_1)\beta\;+\varphi_1(\alpha''_1,\beta''_1,\gamma''_1)\gamma\;=\varphi_1(\alpha_1,\beta_1,\gamma_1).\boldsymbol{A},\\ \varphi_1(\alpha_1,\beta_1,\gamma_1)\alpha'+\varphi_1(\alpha'_1+\beta'+\gamma'_1)\beta'+\varphi_1(\alpha''_1,\beta''_1,\gamma''_1)\gamma'=\varphi_1(\alpha'_1,\beta'_1,\gamma'_1).\boldsymbol{A},\\ \varphi_1(\alpha_1,\beta_1,\gamma_1)\alpha''+\varphi_1(\alpha'_1+\beta'_1+\gamma'_1)\beta''+\varphi_1(\alpha''_1,\beta''_1,\gamma''_1)\gamma''=\varphi_1(\alpha''_1,\beta''_1,\gamma''_1).\boldsymbol{A}.\end{cases}$$

Die Zusammensetzung der Systeme (17.) und (1.) liefert das folgende System:

$$(18^a.)\quad\left\{\begin{matrix}\alpha_2, & \alpha'_2, & \alpha''_2\\ \beta_2, & \beta'_2, & \beta''_2\\ \gamma_2, & \gamma'_2, & \gamma''_2\end{matrix}\right\},$$

wo

$$(19.)\quad\begin{cases}\alpha_2=\alpha_1\alpha+\alpha'_1\beta+\alpha''_1\gamma, & \alpha'_2=\alpha_1\alpha'+\alpha'_1\beta'+\alpha''_1\gamma', & \alpha''_2=\alpha_1\alpha''+\alpha'_1\beta''+\alpha''_1\gamma'',\\ \beta_2=\beta_1\alpha+\beta'_1\beta+\beta''_1\gamma, & \beta'_2=\beta_1\alpha'+\beta'_1\beta'+\beta''_1\gamma', & \beta''_2=\beta_1\alpha''+\beta'_1\beta''+\beta''_1\gamma'',\\ \gamma_2=\gamma_1\alpha+\gamma'_1\beta+\gamma''_1\gamma, & \gamma'_2=\gamma_1\alpha'+\gamma'_1\beta'+\gamma''_1\gamma', & \gamma''_2=\gamma_1\alpha''+\gamma'_1\beta''+\gamma''_1\gamma''\end{cases}$$

ist. Es kommt also jetzt darauf an, die Buchstaben $\alpha, \beta, \gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ aus den Gleichungen (18.) zu bestimmen und ihre Werthe in (19.) zu setzen, oder, was auf dasselbe hinauskommt, die eben geschriebenen Buchstaben auf irgend eine Weise zwischen den Gleichungen (18.) und (19.) zu eliminiren. Diese Elimination ist leicht; denn jene Buchstaben fallen von selbst aus (18.) heraus, wenn man überall links die Multiplication ausführt, und man erhält die einfachen Formeln

$$a_1\alpha_2+\lambda_1\beta_2+\lambda'_1\gamma_2 = \varphi_1(\alpha_1,\beta_1,\gamma_1).\boldsymbol{A},$$
$$a_1\alpha'_2+\lambda_1\beta'_2+\lambda'_1\gamma'_2 = \varphi_1(\alpha'_1,\beta'_1,\gamma'_1).\boldsymbol{A},$$
$$a_1\alpha''_2+\lambda_1\beta''_2+\lambda'_1\gamma''_2 = \varphi_1(\alpha''_1,\beta''_1,\gamma''_1).\boldsymbol{A},$$

oder

$$(20.)\quad\begin{cases}\varphi_1(\alpha_2,\beta_2,\gamma_2) = \varphi_1(\alpha_1,\beta_1,\gamma_1).\boldsymbol{A},\\ \varphi_1(\alpha'_2,\beta'_2,\gamma'_2) = \varphi_1(\alpha'_1,\beta'_1,\gamma'_1).\boldsymbol{A},\\ \varphi_1(\alpha''_2,\beta''_2,\gamma''_2) = \varphi_1(\alpha''_1,\beta''_1,\gamma''_1).\boldsymbol{A}.\end{cases}$$

Diese höchst einfachen Formeln, welche neun Gleichungen repräsentiren, liefern, nach α_2, β_2 u. s. w. aufgelöset, alle Transformationen von $\boldsymbol{F}_1$ in $\boldsymbol{F}$, in eine derselben ausgedrückt. Es erhellet aus dem Gange der Rechnung, dafs $\boldsymbol{A}$ in diesen Formeln dieselbe Bedeutung hat, wie in (16.), und dafs alle Werthe von $\boldsymbol{A}$, welche in (16.) ganze Systeme geben, auch hier in (20.) ganze

Systeme liefern werden, während alle Werthe von A, welche dort gebrochene Systeme geben, auch hier gebrochene Systeme, und zwar mit demselben Generalnenner, wie dort, geben werden; so dafs also dieser letztere immer ein Theiler von a^3 sein wird; endlich, dafs es keine andern Transformationen von F_1 in F giebt, als die in den Formeln (20.) enthaltenen.

Wir wollen jetzt mit Hülfe der Formeln (20.) alle Substitutionen suchen, durch welche *die Form F_1 in sich selbst* übergeht. Offenbar lassen sich nach I. alle diese Substitutionen finden, wenn man alle Substitutionen von F_1 in F (und diese sind durch (20.) gegeben) mit irgend einer bestimmten Substitution von F in F_1 zusammensetzt. Nun ist eine Substitution von F in F_1 gegeben, nämlich die umgekehrte von (17.), d. h. die folgende:

$$\left\{\begin{matrix} \beta'_1\gamma''_1-\beta''_1\gamma'_1, & \alpha''_1\gamma'_1-\alpha'_1\gamma''_1, & \alpha'_1\beta''_1-\alpha''_1\beta'_1 \\ \beta''_1\gamma_1-\beta_1\gamma''_1, & \alpha_1\gamma''_1-\alpha''_1\gamma_1, & \alpha''_1\beta_1-\alpha_1\beta''_1 \\ \beta_1\gamma'_1-\beta'_1\gamma_1, & \alpha'_1\gamma_1-\alpha_1\gamma'_1, & \alpha_1\beta'_1-\alpha'_1\beta_1 \end{matrix}\right\} = \left\{\begin{matrix} \alpha_3, & \alpha'_3, & \alpha''_3 \\ \beta_3, & \beta'_3, & \beta''_3 \\ \gamma_3, & \gamma'_3, & \gamma''_3 \end{matrix}\right\},$$

welche offenbar ganze Coëfficienten hat. Die Substitutionen (18ᵃ.), mit der eben geschriebenen zusammengesetzt, geben

$$\left\{\begin{matrix} \alpha_4, & \alpha'_4, & \alpha''_4 \\ \beta_4, & \beta'_4, & \beta''_4 \\ \gamma_4, & \gamma'_4, & \gamma''_4 \end{matrix}\right\};$$

wo die Gleichungen für α_4, α'_4 u. s. w., welche wir zur Erleichterung des Druckes nicht hinschreiben, leicht nach dem Schema (19.) gebildet werden können; man findet z. B.

$$\alpha_4 = \alpha_2(\beta'_1\gamma''_1-\beta''_1\gamma'_1)+\alpha'_2(\beta''_1\gamma_1-\beta_1\gamma''_1)+\alpha''_2(\beta_1\gamma'_1-\beta'_1\gamma_1)$$

u. s. w. Es handelt sich jetzt darum, aus den eben erwähnten Gleichungen, von denen blofs die erste hingeschrieben ist, und aus den Gleichungen (20.) die Buchstaben α_2, β_2 u. s. w. und, wo möglich, auch die Buchstaben α_1, β_1 u. s. w. zu eliminiren. Diese Elimination ist eben so leicht, wie die weiter oben ausgeführte. In der That: wenn man von den Formeln (20.), d. h. von den Formeln

$$\begin{aligned} a_1\alpha_2+\lambda_1\beta_2+\lambda'_1\gamma_2 &= A(a_1\alpha_1+\lambda_1\beta_1+\lambda'_1\gamma_1), \\ a_1\alpha'_2+\lambda_1\beta'_2+\lambda'_1\gamma'_2 &= A(a_1\alpha'_1+\lambda_1\beta'_1+\lambda'_1\gamma'_1), \\ a_1\alpha''_2+\lambda_1\beta''_2+\lambda'_1\gamma''_2 &= A(a_1\alpha''_1+\lambda_1\beta''_1+\lambda'_1\gamma''_1) \end{aligned}$$

die erste mit α_3, die zweite mit β_3, die dritte mit γ_3 multiplicirt, addirt und bei dieser Addition die einfachsten Eigenschaften der Determinante (des Systems (17.)) berücksichtigt, so erhält man einfach:

$$a_1\alpha_4+\lambda_1\beta_4+\lambda'_1\gamma_4 = a_1A.$$

Multiplicirt man dagegen die erste, zweite, dritte der drei Gleichungen resp. mit α'_3, β'_3, γ'_3 und addirt, so kommt

$$a_1\alpha'_4+\lambda_1\beta'_4+\lambda'_1\gamma'_4 = \lambda_1 A;$$

und multiplicirt man endlich jene drei Gleichungen resp. mit α''_3, β''_3, γ''_3 und addirt, so ergiebt sich

$$a_1\alpha''_4+\lambda_1\beta''_4+\lambda'_1\gamma''_4 = \lambda'_1 A.$$

Durch diese drei Formeln, in welchen alle überflüssigen Buchstaben von selbst herausgefallen sind, und welche sich kürzer so schreiben lassen:

$$(21.)\quad \begin{cases} \varphi_1(\alpha_4,\ \beta_4,\ \gamma_4) = a_1 A, \\ \varphi_1(\alpha'_4,\ \beta'_4,\ \gamma'_4) = \lambda_1 A, \\ \varphi_1(\alpha''_4,\ \beta''_4,\ \gamma''_4) = \lambda'_1 A, \end{cases}$$

werden also, wenn man sie nach α_4 u. s. w. auflöset, alle Substitutionen von F_1 in sich selbst gegeben. In diesen Formeln hat A dieselbe Bedeutung, wie in (20.) und in (16.), und es gilt überhaupt von (21.) Alles, was oben von (20.) gesagt wurde. Man wird bemerken, dafs die Formeln (21.) von der Form F, deren wir zu ihrer Erlangung bedurften, ganz unabhängig sein würden, wenn sie nicht noch durch die Werthe, welche man dem A zu geben hat, mit den Formeln (16.) verknüpft wären. Dieser letztere merkwürdige Umstand wird jetzt dazu dienen, die beiden oben in II. gemachten Behauptungen vollständig zu erweisen und dadurch alle Resultate von der Unsicherheit zu befreien, mit welcher sie bis jetzt behaftet waren, und welche darin bestand, dafs man nicht genau wufste, welche Werthe U, V, W, also auch A, in den Gleichungen (16.) erhalten müssen, damit diese Gleichungen ganze Werthe für die Transformationscoëfficienten α, β u. s. w. liefern.

In der That: da wir bisher gar keine weitere Annahme über die Form F_1 gemacht haben, als dafs dieselbe der Form F aequivalent sein soll, und da nach §. 7. I. immer Zahlen durch F dargestellt werden können, welche zu einer beliebigen Zahl z. B. a relative Primzahlen sind: da folglich nach §. 6. F immer in eine aequivalente Form transformirt werden kann, deren erster Coëfficient zu a relative Primzahl ist: so kann man annehmen, *dafs a_1 zu a relative Primzahl ist.* Diese Annahme werde gemacht. Bestimmen wir jetzt, ohne alle Rücksicht auf das Vorhergehende und unabhängig von den Formeln (21.), blofs nach Anleitung von II. dieses Paragraphen, alle Substitutionen von F_1 in sich selbst, so findet sich, dafs dieselben in den folgenden Formeln enthalten sind:

$$(22.)\quad\begin{cases}\varphi_1(\alpha_4,\ \beta_4,\ \gamma_4) = a_1 A_4,\\ \varphi_1(\alpha_4',\ \beta_4',\ \gamma_4') = \lambda_1 A_4,\\ \varphi_1(\alpha_4'',\ \beta_4'',\ \gamma_4'') = \lambda_1' A_4,\end{cases}$$

wo $A_4 = U_4 + (V_4 + W_4\varrho)\eta + (V_4 + W_4\varrho^2)\vartheta$, und U_4, V_4, W_4 alle rationalen Zahlen mit dem Nenner a_1 oder einem Theiler von a_1 vorstellen, die der Gleichung (4.) genügen. Wäre es nun, gegen unsere erste oben in II. aufgestellte Behauptung, möglich, dafs gebrochene Werthe von U, V, W (mit dem Nenner a oder einem Theiler von a) in den Formeln (16.) ganze Systeme lieferten, so müfsten auch in den Gleichungen (21.) dieselben gebrochenen Werthe von U, V, W ganze Systeme für α_4, β_4 u. s. w. geben; diese speciellen ganzen Systeme können aber offenbar in den Gleichungen (22.) nicht enthalten sein, weil dort U_4, V_4, W_4 nur Nenner erhalten, welche Theiler von a_1 sind, und a und a_1 keinen gemeinschaftlichen Theiler haben; also müfste es ganze Systeme für α_4, β_4 u. s. w. geben, die in den Formeln (22.) nicht enthalten wären; was dem oben in II. Bewiesenen widerspricht. Es müssen also nothwendig von den Formeln (16.), also auch von den Formeln (20.) und (21.), alle gebrochenen Werthe von U, V, W ausgeschlossen werden: also müssen auch von den Formeln (22.) alle gebrochenen Werthe von U_4, V_4, W_4 ausgeschlossen werden. Zweitens ist zu beweisen, dafs für alle ganzen Werthe von U, V, W die Formel (16.) immer ganze Werthe der Transformationscoëfficienten liefert. Wäre es möglich, dafs einem bestimmten Systeme ganzer Werthe von U, V, W in (16.) gebrochene Werthe der Transformationscoëfficienten entsprächen, so könnte der Generalnenner dieser letzteren doch nur ein Theiler von a^3 sein, und derselbe Generalnenner müfste sich zu demselben System U, V, W, für die Transformationscoëfficienten α_4, β_4 u. s. w. aus (21.) ergeben. Aber wenn man, was erlaubt ist, in den Formeln (22.) $U_4 = U$, $V_4 = V$, $W_4 = W$, d. h. diesem speciellen Systeme gleichsetzt, welches wir jetzt gerade im Auge haben, so folgt aus diesen Formeln (22.) nach II., dafs der Generalnenner von α_4, β_4 u. s. w. nur ein Theiler von a_1^3 sein kann; es müfste also der Generalnenner dieser Zahlen α_4, β_4 u. s. w. zugleich ein Theiler von a^3, nach (21.), und zugleich, nach (22.), ein Theiler von a_1^3 sein; was sich widerspricht, da a und a_1 relative Primzahlen sind.

Da die beiden Behauptungen in II. jetzt unzweifelhaft bewiesen sind, so können wir die gewonnenen Resultate vervollständigen, indem wir hinzufügen, dafs in den Formeln (16.), (20.), (21.), (22.) U, V, W nur ganze Werthe vorstellen und dafs alle ganzen Systeme U, V, W, welche der Glei-

chung (4.) genügen, nach und nach in diese Formeln gesetzt, immer ganze Werthe der Transformationscoëfficienten liefern. Nach dieser Bemerkung fallen die Formeln (21.) und (22.) als identisch zusammen und drücken nichts anderes für die Form F_1 aus, als was durch (16.) schon für die Form F gegeben ist, während die Formeln (20.) ihrerseits wieder (16.) als speciellen Fall enthalten, wenn man für das System (17.) das folgende annimmt:

$$\left\{\begin{matrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}\right\},$$

durch welches jede Form in sich selbst übergeht. Wir können daher folgenden merkwürdigen Fundamentalsatz für die Transformation der associirten Formen aufstellen.

Lehrsatz 6.

„Wenn zwei aequivalente Formen F und G durch die Substitution $\left\{\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}\right\}$ in einander übergehen, und man setzt

$$a^2 F = \varphi(u, v, w)\,\psi(u, v, w)\,\chi(u, v, w),$$

so erhält man alle möglichen Substitutionen von F in G aus den Formeln

$$(\text{I.})\quad \left\{\begin{aligned} \varphi(\alpha_1, \beta_1, \gamma_1) &= \varphi(\alpha, \beta, \gamma)(U + Y\eta + Z\vartheta), \\ \varphi(\alpha'_1, \beta'_1, \gamma'_1) &= \varphi(\alpha', \beta', \gamma')(U + Y\eta + Z\vartheta), \\ \varphi(\alpha''_1, \beta''_1, \gamma''_1) &= \varphi(\alpha'', \beta'', \gamma'')(U + Y\eta + Z\vartheta), \end{aligned}\right.$$

$$Y = V + W\varrho, \quad Z = V + W\varrho^2,$$

wenn man nach und nach in diese Formeln statt U, V, W alle reellen ganzen Zahlen einführt, die der Gleichung

$$(\text{II.})\quad U^3 + pp_1 Y^3 + pp_2 Z^3 - 3p\,UYZ = 1$$

genügen (deren allgemeine Lösung in §. 4. gegeben wurde), und wenn man für jedes System von Lösungen dieser unbestimmten Gleichung aus den neun in (I.) implicite enthaltenen Gleichungen die Werthe von α_1, β_1 u. s. w. bestimmt, welche sich aus diesen neun Gleichungen immer als ganze Zahlen ergeben."

Vermöge dieses Resultats läfst sich die Lösung aller bisher behandelten Fragen vervollständigen. Dies wird der Gegenstand des folgenden Paragraphen sein.

§. 9.

Wir beschäftigen uns zuerst mit derjenigen Frage, welche die Darstellung der Zahlen betrifft. Damit eine gegebene positive Zahl M durch eine

ebenfalls gegebene associirte Form F (eigentlich) darstellbar sei, ist es nach §. 6. erforderlich und hinreichend, dafs eine reducirte Form mit dem ersten Coëfficienten M existirt, die der Form F aequivalent ist; und aus jeder reducirten Form dieser Art leitet man eine Gruppe von Darstellungen ab, indem man nach und nach die Variabeln der Form F resp. den drei ersten Coëfficienten in allen möglichen Substitutionen gleich setzt, welche F in diese bestimmte reducirte Form verwandeln. Es sei α, β, γ eine specielle Darstellung von M durch F, so dafs also nothwendig F durch eine Substitution, deren erste Coëfficienten α, β, γ sind, in eine reducirte Form mit dem ersten Coëfficienten M übergeht. Um alle Darstellungen derselben Gruppe zu finden, ist nur nöthig, alle Substitutionen aufzusuchen, welche dieselbe Wirkung hervorbringen, oder vielmehr, nur alle ersten Coëfficienten dieser Substitutionen. Diese ersten Coëfficienten sind nach dem vorigen Paragraphen durch die folgende Formel gegeben:

$$(1.)\quad \varphi(\alpha_1, \beta_1, \gamma_1) = \varphi(\alpha, \beta, \gamma)(U + Y\eta + Z\vartheta),$$

wo, wie oben,

$$a^2 F = \varphi(u, v, w)\,\psi(u, v, w)\,\chi(u, v, w) \text{ ist.}$$

Diese Formel, welche implicite 3 Gleichungen enthält, liefert, durch die Auflösung dieser 3 Gleichungen nach α_1, β_1, γ_1 für jede Lösung der unbestimmten Gleichung $\Phi = 1$ (II.), alle Darstellungen α_1, β_1, γ_1 einer Gruppe, in eine specielle α, β, γ derselben Gruppe ausgedrückt.

Setzt man der Kürze wegen

$$U + Y\eta + Z\vartheta = A$$

und die beiden correspondirenden Ausdrücke $= B$ und $= C$, und bezeichnet diejenigen Werthe von A, B, C, welche einer Fundamental-Auflösung der Gleichung $\Phi = 1$ entsprechen, durch

$$\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C},$$

so sind nach §. 4. alle Werthe von A durch die Formel

$$A = \mathfrak{A}^m \mathfrak{B}^n$$

gegeben; wo m und n alle ganzen Werthe von $-\infty$ bis $+\infty$ durchlaufen: also erhält man

$$(2.)\quad \varphi(\alpha_1, \beta_1, \gamma_1) = \varphi(\alpha, \beta, \gamma)\,\mathfrak{A}^m \mathfrak{B}^n = \varphi(\alpha, \beta, \gamma)\,A.$$

Es werde, um abzukürzen,

$$\varphi(\alpha_1, \beta_1, \gamma_1) = \varphi, \quad \psi(\alpha_1, \beta_1, \gamma_1) = \psi, \quad \chi(\alpha_1, \beta_1, \gamma_1) = \chi,$$
$$\varphi(\alpha, \beta, \gamma) = \varphi_0, \quad \psi(\alpha, \beta, \gamma) = \psi_0, \quad \chi(\alpha, \beta, \gamma) = \chi_0$$

gesetzt. Bedient man sich der Characteristik Log in demselben Sinne, wie in

§. 4., nämlich um den natürlichen Logarithmen des absoluten Werthes einer reellen Zahl auszudrücken, so geben die Gleichung

$$\varphi = \varphi_0 . A \text{ und ihre correspondirende } \psi = \psi_0 . B:$$

$$\operatorname{Log}\varphi - \varrho \operatorname{Log}\psi = \operatorname{Log}\varphi_0 - \varrho \operatorname{Log}\psi_0 + \operatorname{Log} A - \varrho \operatorname{Log} B.$$

Aber alle Werthe von $\operatorname{Log} A - \varrho \operatorname{Log} B$ sind nach §. 4. durch die Formel

$$\operatorname{Log} A - \varrho \operatorname{Log} B = (m + n\varrho)(\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B})$$

gegeben, also kommt

$$\operatorname{Log}\varphi - \varrho \operatorname{Log}\psi = \operatorname{Log}\varphi_0 - \varrho \operatorname{Log}\psi_0 + (m + n\varrho)(\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B})$$

oder

$$(3.) \quad \frac{\operatorname{Log}\varphi - \varrho \operatorname{Log}\psi}{\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B}} = m + n\varrho + \frac{\operatorname{Log}\varphi_0 - \varrho \operatorname{Log}\psi_0}{\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B}}$$

Die Gleichung (3.) ist eine nothwendige Folge von (2.); aber ebenso ist umgekehrt (2.) eine nothwendige Folge von (3.); folglich giebt (3.), ebensowohl wie (2.), alle Darstellungen einer Gruppe von M durch F, und jede nur einmal.

Stellt man sich die beiden Quotienten rechts und links in (3.) auf die Form $\mu + \nu\varrho$ gebracht vor, so sieht man, dafs ein, und nur ein Werth von m, und ein, und nur ein Werth von n existirt, welcher macht, dafs der reelle Theil sowohl, als der Coëfficient von ϱ in dem Quotienten links, $\geqq 0$ und < 1 wird; es giebt also *eine* und *nur eine* Darstellung in jeder Gruppe, für welche diese letztere Bedingung erfüllt wird.

Wenn man, ehe man die Logarithmen nimmt, die Gleichungen $\varphi = \varphi_0 . A$, $\psi = \psi_0 . B$ erst mit einer beliebigen positiven Constante k multiplicirt, so erhält man statt der Gleichung (3.) die folgende:

$$(4.) \quad \frac{\operatorname{Log}(k\varphi) - \varrho \operatorname{Log}(k\psi)}{\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B}} = m + n\varrho + \frac{\operatorname{Log}(k\varphi_0) - \varrho \operatorname{Log}(k\psi_0)}{\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B}};$$

und in dieser Gleichung giebt es ebenfalls immer ein, und nur ein System m, n, für welches der reelle Theil und der Coëfficient von ϱ des Quotienten links $\geqq 0$ und < 1 ist. Nun sind der reelle Theil und der Coëfficient von ϱ in diesem Quotienten resp. gleich

$$\frac{1}{\sigma}[(\operatorname{Log}\mathfrak{A} + \operatorname{Log}\mathfrak{B}) \operatorname{Log}(k\varphi) + \operatorname{Log}\mathfrak{B} . \operatorname{Log}(k\psi)],$$

$$\frac{1}{\sigma}[\operatorname{Log}\mathfrak{B} . \operatorname{Log}(k\varphi) - \operatorname{Log}\mathfrak{A} . \operatorname{Log}(k\psi)],$$

wo

$$\sigma = (\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B})(\operatorname{Log}\mathfrak{A} - \varrho^2 \operatorname{Log}\mathfrak{B}) = N(\operatorname{Log}\mathfrak{A} - \varrho \operatorname{Log}\mathfrak{B})$$

wie in §. 4. die Norm des Regulators der Fundamental-Auflösungen der Gleichung $\Phi = 1$ bezeichnet, also das *Minimum* unter allen Werthen, welche

$N(\text{Log}\,A - \varrho\,\text{Log}\,B)$ erhalten kann. Diese vollkommen bestimmte, immer positive und nur von dem Werthe der Primzahl p abhängige Constante σ wird oft in den nachfolgenden Untersuchungen erscheinen. Wir schliefsen hieraus folgenden Satz.

Lehrsatz 7.

„*Unter der Totalität der Darstellungen einer Gruppe befindet sich immer eine, und nur eine, für welche die Bedingungen*

$$(5.)\quad \begin{cases} 0 \leqq (\text{Log}\,\mathfrak{A} + \text{Log}\,\mathfrak{B})\,\text{Log}(k\varphi) + \text{Log}\,\mathfrak{B}\,.\,\text{Log}(k\psi) < \sigma, \\ 0 \leqq \text{Log}\,\mathfrak{B}\,.\,\text{Log}(k\varphi) - \text{Log}\,\mathfrak{A}\,.\,\text{Log}(k\psi) < \sigma \end{cases}$$

erfüllt werden, während k eine beliebige positive Constante bezeichnet."

Es ist gut, zu bemerken, dafs die Constante k, obwohl unabhängig von den Variabeln der Form F, doch als eine Function von M und von beliebigen andern Zahlen angesehen werden kann, und dafs die Darstellung, welche vermöge der Ungleichheitsbedingungen (5.) aus ihrer ganzen Gruppe herausgehoben wird, mit dem Werthe von k *variirt.*

Man betrachte noch einmal die Gleichung (4.). Aufser dem vorhin berücksichtigten System m, n giebt es noch ein anderes, welches ebenfalls eine merkwürdige Eigenschaft hat; nämlich dasjenige, welches bewirkt, dafs der reelle Theil und der Coëfficient von ϱ links beide ihrem *absolutem* Werthe nach $\leqq \frac{1}{2}$ werden; für dieses System m, n wird offenbar die Norm des Quotienten links in (4.) $\leqq \frac{3}{4}$, also kommt

$$(6.)\quad N(\text{Log}(k\varphi) - \varrho\,\text{Log}(k\psi)) \leqq \tfrac{3}{4}\sigma.$$

Es giebt also immer Darstellungen in jeder Gruppe, für welche dieser letzteren Bedingung (6.) genügt wird, obgleich sich nicht behaupten läfst, dafs es nur eine solche Darstellung giebt: diesen Vorzug besitzen nur die Bedingungen (5.), während es in Hinsicht auf (6.) je nach der Natur der Gruppe *eine, zwei,* oder *drei,* aber nie mehr, ihr genügende Darstellungen geben kann. Dieser Umstand hängt mit einer Eigenschaft einer Ellipse zusammen, deren Gleichung zwischen rechtwinkligen Coordinaten $x^2 + xy + y^2 = \frac{3}{4}$ ist, nemlich, dafs sie, auf ein *Gitter,* wie es in der Abhandlung „Geometrischer Beweis u. s. w." definirt wurde, in verschiedenen Lagen und Verschiebungen gezeichnet, bald *einen,* bald *zwei,* bald *drei* Gitterpuncte, aber nie mehr, in ihre Fläche aufnehmen kann. Es wäre interessant, im Allgemeinen die *Wahrscheinlichkeit* anzugeben, welche jeder dieser drei Fälle hat.

Aufgabe. „Es ist eine positive ganze Zahl M und eine associirte Form F gegeben: man soll entscheiden, ob M durch F darstellbar sei, oder

nicht; und man soll im ersten dieser beiden Fälle alle Darstellungen angeben, deren M durch diese Form fähig ist."

Nach dem Lehrsatze 7. kommt die Aufgabe offenbar darauf hinaus, zu untersuchen, ob es ganze Werthe ohne gemeinschaftlichen Theiler der Variabeln der Form giebt, für welche die Bedingung

$$(7.)\qquad \varphi\psi\chi = a^2 M$$

und zugleich die Bedingungen (5) erfüllt werden: existiren gar keine solchen Werthe, so giebt es auch keine Darstellungen von M durch F; im entgegengesetzten Falle liefert jedes diesen Bedingungen genügende System von Werthen der Variabeln, statt α, β, γ in die Formel (2.) gesetzt, eine Gruppe von Darstellungen; alle diese Gruppen werden verschieden sein, und es kann keine Gruppen geben, die nicht auf diese Art gefunden würden. Alles kommt also darauf an, den Bedingungen (5.) und (7.) gleichzeitig zu genügen.

Die Ungleichheiten (5.) geben

$$N(\mathrm{Log}(k\varphi)-\varrho\,\mathrm{Log}(k\psi)) < 2\sigma.$$

Da diese Bedingung sich auch auf die beiden folgenden Arten schreiben läfst:

$$\{\mathrm{Log}(k\varphi)+2\,\mathrm{Log}(k\psi)\}^2+3\,\mathrm{Log}(k\varphi)^2 < 8\sigma,$$
$$\{2\,\mathrm{Log}(k\varphi)+\mathrm{Log}(k\psi)\}^2+3\,\mathrm{Log}(k\psi)^2 < 8\sigma,$$

so hat man um so mehr noch

$$\mathrm{Log}(k\varphi)^2 < \tfrac{8}{3}\sigma,\qquad \mathrm{Log}(k\psi)^2 < \tfrac{8}{3}\sigma,$$

folglich

$$-\sqrt{(\tfrac{8}{3}\sigma)} < \mathrm{Log}(k\varphi) < \sqrt{(\tfrac{8}{3}\sigma)},\qquad -\sqrt{(\tfrac{8}{3}\sigma)} < \mathrm{Log}(k\psi) < \sqrt{(\tfrac{8}{3}\sigma)}.$$

Durch diese letzteren Bedingungen sind ganz bestimmte untere und obere Grenzen für die ***absoluten*** Werthe (d. h. ohne Rücksicht auf das Vorzeichen) von φ und ψ gegeben, also auch für den absoluten Werth von $\frac{1}{\varphi\psi}$; aber aus (7.) folgt $\chi = \frac{a^2 M}{\varphi\psi}$, mithin liegt auch $\pm.\chi$ zwischen einer ganz bestimmten untern und obern Grenze. Diese Grenzen seien für den absoluten Werth von φ der Kürze wegen durch λ, λ', für den von ψ durch μ, μ', für den von χ durch ν, ν' bezeichnet, wo dann λ, λ', μ, μ', ν, ν' vollkommen bestimmte positive Constanten und zwar Exponentialfunctionen von σ sein werden. Da nun $\varphi\psi\chi = a^2 M$, also immer positiv ist, so lassen sich für φ, ψ, χ nur folgende Zeichencombinationen denken:

$$+,\ +,\ +;\quad +,\ -,\ -;\quad -,\ +,\ -;\quad -,\ -,\ +.$$

Also sind folgende vier Systeme von Ungleichheiten zu berücksichtigen:

$$\begin{array}{c|c|c|c} \lambda<\varphi<\lambda' & \lambda<\varphi<\lambda' & -\lambda'<\varphi<-\lambda & -\lambda'<\varphi<-\lambda \\ \mu<\psi<\mu' & -\mu'<\psi<-\mu & \mu<\psi<\mu' & -\mu'<\psi<-\mu \\ \nu<\chi<\nu' & -\nu'<\chi<-\nu & -\nu'<\chi<-\nu & \nu<\chi<\nu'; \end{array}$$

und da alle vier dieselbe Behandlung zulassen, so betrachten wir nur das erste. Da φ, ψ, χ offenbar lineare homogene Functionen der Variabeln von der Form F mit *reellen* Coëfficienten sind, so kommt jetzt Alles darauf an, eine Regel anzugeben, nach welcher sich aus einem System von Ungleichheiten von der Form

$$(\Omega.)\quad \begin{cases} \lambda < \alpha u+\alpha' v+\alpha'' w < \lambda', \\ \mu < \beta u+\beta' v+\beta'' w < \mu', \\ \nu < \gamma u+\gamma' v+\gamma'' w < \nu' \end{cases}$$

alle ganzen Werthe für u, v, w finden lassen, welche demselben genügen; $\alpha, \alpha', \alpha'', \beta$ u. s. w. sind gegebene reelle Werthe. Man sieht zunächst, dafs die Anzahl dieser ganzen Systeme u, v, w immer endlich sein wird: denn betrachtet man das Problem als ein geometrisches, so sieht man, dafs alle Puncte u, v, w (auf rechtwinklige Coordinaten bezogen), für welche diese drei Bedingungen erfüllt sind, innerhalb eines *Parallelepipedums* liegen, dessen parallele Seiten-Ebenen durch die Gleichungen

$$\begin{array}{lll} \alpha u+\alpha' v+\alpha'' w = \lambda & \text{und} & = \lambda', \\ \beta u+\beta' v+\beta'' w = \mu & \text{und} & = \mu', \\ \gamma u+\gamma' v+\gamma'' w = \nu & \text{und} & = \nu' \end{array}$$

resp. gegeben sind; so dafs also weiter nichts verlangt wird, als alle innerhalb dieses Parallelepipedums liegenden Würfelpuncte (vergl. §. 4. IV.) zu finden. Man könnte hierauf eine Lösung gründen, indem man nach geometrischen Principïen die am weitesten hinausliegenden Puncte des Parallelepipedums nach oben und nach unten, nach vorn und nach hinten, nach rechts und nach links suchte, und daraus Grenzen für u, v, w selbst erhielte; aber wir wollen das Problem rein analytisch behandeln. Man eliminire aus den obigen Ungleichheiten, ganz auf dieselbe Weise wie bei einem linearen System von Gleichungen, vermittels der bekannten Methode der Multiplicatoren nach und nach je zwei von den drei Variabeln, wobei man nur die Vorsicht zu beobachten hat, dafs man, wenn ein Multiplicator *negativ* ist, alle Zeichen $<$ in $>$ verwandele, oder, was für die practische Ausführung am bequemsten ist, dafs man in diesem Falle die drei Glieder, aus denen die Ungleichheit zusammengesetzt ist, in umgekehrter Ordnung schreibe, so dafs man z. B., wenn man v und w eliminiren will, und der Multiplicator $\beta'\gamma''-\beta''\gamma'$ negativ ist, als erste Zeile

$$(\beta'\gamma''-\beta''\gamma')\lambda' < (\beta'\gamma''-\beta''\gamma')\alpha u + \text{etc.} < (\beta'\gamma''-\beta''\gamma')\lambda$$

zu schreiben hat. Beobachtet man dieses Verfahren, indem man jede der drei Ungleichheiten mit geeigneten Multiplicatoren multiplicirt, und addirt dann jedesmal die Resultate, so wird man zu drei Ungleichheiten von der Form

$$A < u < A', \quad A_1 < v < A_1', \quad A_2 < w < A_2'$$

geführt, welche eine nothwendige Folge der obigen sind; so dafs nun die ganzen Werthe von u, v, w in vollkommen bestimmte Grenzen eingeschlossen sind. Man beachte, dafs diese Methode ebenso auf lineare Ungleichheiten mit beliebig vielen Variabeln angewandt werden kann, und dafs auch hier, wie bei den Gleichungen, die hinreichende Bedingung der Möglichkeit der Lösung darin besteht, dafs die Determinante des Systems einen von Null verschiedenen Werth haben mufs; diese Bedingung wird bei unsern vier obigen Systemen erfüllt, weil ihre Determinante, wie schon öfter bemerkt, $= -9pa^2$ ist.

Von den auf diese Weise aus den vier obigen Systemen gefundenen ganzen Werthen für u, v, w müssen zuerst diejenigen ausgeschlossen werden, welche einen gemeinschaftlichen Theiler haben; alle übrigen müssen in die beiden Bedingungen (5.) und (7.) eingesetzt werden; alle diejenigen von ihnen, welche diesen beiden Bedingungen zugleich genügen, geben ebenso viele Lösungen der Aufgabe; alle übrigen sind zu verwerfen. — Wir kommen jetzt zu der Aequivalenz der Formen.

Aufgabe. „Es sind zwei associirte Formen F und G gegeben: man soll entscheiden, ob dieselben aequivalent sind, oder nicht, und im ersten Falle alle Transformationen von F in G suchen."

Es sei a der erste Coëfficient von F; man verwandle nach Anleitung von §. 6. F in eine reducirte Form mit dem ersten Coëfficienten a; diese sei R. Je nachdem nun G und R aequivalent sind, oder nicht, werden auch F und G aequivalent sein, oder nicht. Damit aber G und R aequivalent seien, ist nach §. 6. erforderlich und hinreichend, dafs es eine Darstellung von a durch G gebe, deren Gruppe zu der reducirten Form R gehört. Man suche folglich nach der vorigen Aufgabe alle Gruppen von Darstellungen der Zahl a durch die Form G, oder vielmehr aus jeder Gruppe eine dieser Darstellungen; zu jeder der so gefundenen Darstellungen α, β, γ, deren Anzahl offenbar endlich ist, bestimme man nach §. 6. sechs ganze Zahlen α', β', γ', α'', β'', γ'', von der Art, dafs die Determinante des Systems

$$\left\{\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}\right\}$$

der Einheit gleich wird, und dafs G durch die eben geschriebene Substitution in eine reducirte Form mit dem ersten Coëfficienten a übergeht. Diese Operation, der Reihe nach auf alle gefundenen Darstellungen angewandt, liefert offenbar nach §. 6. alle zu a gehörigen und der Form G aequivalenten reducirten Formen. Wir haben also nur noch zu untersuchen, ob sich unter diesen reducirten Formen eine befindet, welche mit R identisch ist. Ist dies der Fall, so liefert die hiernach bereits bekannte Substitution S von G in R, in Verbindung mit der ebenfalls bekannten T von F in R, eine Substitution von F in G, nämlich die Substitution $T\times\frac{1}{S}$, aus welcher sich vermöge der Formeln des §. 8. alle übrigen berechnen lassen. Im entgegengesetzten Falle, d. h. wenn *keine* der zuletzt erwähnten reducirten Formen mit R identisch ist, können auch F und G nicht aequivalent sein.

Man sieht, dafs die Beantwortung aller eben behandelten Fragen von der Kenntnifs einer Fundamental-Auflösung der Gleichung $\Phi=1$, d. h. der Gleichung

$$(8.)\qquad u^3+pp_1y^3+pp_2z^3-3puyz = 1,$$
$$y=v+w\varrho,\qquad z=v+w\varrho^2,$$

abhängt. Es wird daher gut sein, eine, wenigstens theoretisch ausführbare, wenn auch nicht in practischer Hinsicht zweckmäfsige Operation anzugeben, durch welche man eine Fundamental-Auflösung dieser Gleichung finden kann.

Es sei u, v, w irgend eine Lösung der Gleichung (8.), welche man auf einem beliebigen Wege, z. B. durch die Principien der Kreistheilung, nach §. 4. III. suchen kann, deren Auffindung also immer möglich ist; es seien A_0, B_0, C_0 die dieser speciellen Auflösung entsprechenden Werthe der drei correspondirenden Linearfactoren von Φ, und es werde der hiernach vollkommen bekannte Ausdruck

$$N(\operatorname{Log}A_0-\varrho\operatorname{Log}B_0),\quad =\tau$$

gesetzt. Um nun eine Fundamental-Auflösung zu finden, haben wir zufolge der Definition derselben nichts anders zu thun, als diejenigen ganzen Werthe von u, v, w zu suchen, für welche erstlich die Norm des Regulators $\leqq\tau$, also

$$(9.)\qquad N(\operatorname{Log}A-\varrho\operatorname{Log}B)\leqq\tau$$

wird; welche Werthe zweitens der Gleichung (8.) genügen, so dafs also

$$(10.)\qquad ABC = 1$$

ist, und für welche aufserdem drittens die Norm des Regulators ein *Minimum* wird. Eine nothwendige Folge der Bedingung (9.) ist $(\operatorname{Log}A)^2<\frac{4}{3}\tau$, $(\operatorname{Log}B)^2<\frac{4}{3}\tau$, folglich

$$-\sqrt{(\tfrac{4}{3}\tau)}<\operatorname{Log}A<\sqrt{(\tfrac{4}{3}\tau)},\qquad -\sqrt{(\tfrac{4}{3}\tau)}<\operatorname{Log}B<\sqrt{(\tfrac{4}{3}\tau)}.$$

Dadurch ergeben sich, wenn man von den Logarithmen zu A und B selbst übergeht, ganz bestimmte positive obere und untere Grenzen für die absoluten Werthe von A und B; also wegen $C = \frac{1}{AB}$ ergeben sich auch ganz bestimmte untere und obere Grenzen für den absoluten Werth von C. Diese Grenzen sind für A und B dieselben, nämlich $e^{-\sqrt{(\frac{4}{3}\tau)}}$, $e^{\sqrt{(\frac{4}{3}\tau)}}$, und $e^{\mp\sqrt{(\frac{1}{3}\tau)}}$ für C, wo e für einen Augenblick die Basis der natürlichen Logarithmen bezeichnet. Man erhält hieraus für A, B, C selbst vier Systeme von Ungleichheiten, die alle von der Form derer in (Ω.) sind und folglich nach der obigen Regel aufgelöset werden können. Hieraus ergeben sich Grenzen für u, v, w, und alle zwischen ihnen enthaltenen ganzen Werthe dieser Variabeln müssen nach und nach in (8.) gesetzt werden. Nachdem man alle diejenigen, für welche letztere Gleichung nicht erfüllt wird, verworfen hat, bilde man die Normen der Regulatoren für alle übrigen; die *kleinste* unter diesen Normen wird $= \sigma$ sein, und die ihr entsprechenden Lösungen sind die Fundamental-Auflösungen.

(Der Schlufs folgt.)

25.

Elementare Lösung einer Aufgabe über das ebene und sphärische Dreieck.

(Von Herrn *J. Steiner*, Professor an der Universität zu Berlin.)

Eine elementare Aufgabe über das geradlinige Dreieck, die mir im Jahr 1840 von Herrn Prof. *Lehmus* mit dem Wunsche zukam: *„eine rein geometrische Lösung derselben zu finden"* und die ich später gelegentlich Andern als Übungsbeispiel mittheilte, ist in neuester Zeit in verschiedenen Druckschriften öffentlich zur Sprache gebracht und gelöset worden. Irrthümlicherweise wurde aber die Aufgabe theils mir zugeschrieben, theils nicht so elementar gelöset, als der Urheber derselben und ich es verlangten; auch wurde der Gegenstand mit solchen Bemerkungen begleitet, welche meine einfache Absicht, die ich bei gesprächsweiser Mittheilung der Aufgabe hatte, weit übertreffen. Dies veranlafst mich — um Mifsverständnisse zu verhindern — meine eigene Lösung der Aufgabe, welche ich damals gefunden und Herrn *Lehmus* sogleich mittheilte, hier nachträglich zu veröffentlichen; zumal da ein grofser Kenner der Geometrie, Herr *Sturm*, der von seinen Zuhörern und Andern verschiedene Lösungen besafs, die meinige für die elementarste hielt. Bei dieser Gelegenheit werde ich zugleich auf die Gründe aufmerksam machen, warum die Aufgabe für die Rechnung umständlicher ausfällt, als man auf den ersten Blick vermuthet; so wie auch die Aufgabe etwas allgemeiner fassen, und zuletzt auch die analoge sphärische Aufgabe behandeln.

Aufgabe I.

„Wenn in einem geradlinigen Dreieck die zwei Geraden, welche dessen Winkel an der Grundlinie hälften und die bis an die Gegenseiten verlängert genommen werden, gleich lang sind, so ist die Frage, ob dann das Dreieck gleichschenklig sei?"

Wenn also z. B. in dem Dreiecke ACB (Fig. 1. Taf. III.) Winkel $\alpha = \alpha_1$, Winkel $\beta = \beta_1$ und die Gerade $AD = BE$ oder $a = b$, so ist die Frage, ob $AC = BC$ oder, was auf dasselbe hinausläuft, ob $\alpha = \beta$ sei?

Wollte man annehmen, die Winkel α und β können ungleich sein, etwa $\alpha > \beta$ (also auch $\alpha_1 > \beta_1$), so zeigt sich die Unmöglichkeit leicht wie folgt.

Vermöge der Dreiecke ADB und BEA, die nach Voraussetzung zwei Paar gleiche Seiten und dazwischen die ungleichen Winkel α und β haben, folgt, dafs $BD > AE$ oder $d > e$ und Winkel $ADB > BEA$ (weil $\alpha_1 + \alpha + \beta > \beta_1 + \beta + \alpha$). Diese Dreiecke denke man sich für einen Augenblick (zur bequemeren Übersicht) in solche Lage gebracht (Fig. 2.), wo sie auf entgegengesetzten Seiten über derselben Grundlinie $c = AB$ stehen und wo die Seiten den durch dieselben Buchstaben bezeichneten in Fig. 1. gleich sind. Da nach der Annahme $a = b$ (d. i. $AD = BE$ Fig. 1.), so ist, wenn man die Gerade DE zieht, Winkel $n = m$, und daher, da Winkel $D > E$ (d. i. Winkel $ADB > BEA$ Fig. 1.), auch Winkel $x > y$; woraus folgt, dafs $e > d$ sein mufs; was dem Vorigen, $d > e$, widerspricht: demnach können α und β nicht ungleich, und folglich mufs das vorgelegte Dreieck ACB gleichschenklig sein.

Dieses ist meine oben erwähnte erste Lösung der Aufgabe. Die Schwierigkeit, welche die Aufgabe bei anderer Behandlung darbietet, mag ihren Grund darin haben, dafs die eine Voraussetzung nicht so absolut bestimmt ist, wie man auf den ersten Blick leicht glauben möchte. Denn wenn gesagt wird: *„die Winkel an der Grundlinie werden gehälftet,"* so ist dies sowohl auf die *inneren* als auf die *äufseren* Winkel an der Grundlinie anzuwenden; was dann im Wesentlichen drei verschiedene Fälle giebt, indem nämlich, wenn man die bis an die Gegenseiten verlängerten Strahlen, welche die innern Winkel hälften durch a und b, und diejenigen, welche die äufseren Winkel hälften, durch a_1 und b_1 bezeichnet, entweder

1. $a = b$, oder
2. $a_1 = b_1$, oder
3. $\begin{cases} a = b_1, \text{ oder} \\ a_1 = b \end{cases}$

angenommen werden kann. Im ersten Falle (1.) ist nun, zufolge des obigen Beweises, das Dreieck allemal gleichschenklig. Beim zweiten Falle (2.) kommt es noch auf eine nähere Unterscheidung an, ob nämlich α) beide Strahlen a_1, b_1 die verlängerten Gegenseiten jenseits der Spitze C, oder beide dieselben unterhalb der Grundlinie AB treffen, oder ob β) der eine die Gegenseite jenseits der Spitze und der andere sie unterhalb der Grundlinie trifft. Unter der Bedingung (α.) ist das Dreieck gleichschenklig; dagegen unter (β.) nicht. Im drit-

ten Falle (3.) endlich ist das Dreieck im Allgemeinen nicht gleichschenklig, (nur scheint die Möglichkeit vorhanden zu sein, dafs es in ganz besonderem Falle gleichschenklig sein kann, wobei es dann aber ein der Form nach ganz bestimmtes Dreieck ist, d. h. bestimmte Winkel hat).

Da nun die Aufgabe alle diese Fälle für die Rechnung stillschweigend zugleich umfafst, so begreift man, wie diese, wenn sie nicht geschickt angegriffen wird, auf höhere Gleichungen führen mufs.

Für den genannten Fall (α), mit der Bedingung, dafs beide Strahlen a_1, b_1 die Gegenseiten jenseits der Spitze C treffen, ist der Beweis dem obigen fast gleich.

Nämlich wollte man annehmen es sei $\alpha_1 > \beta_1$ (Fig. 3.), so wäre $p+\beta > q+\alpha$, und daher $AE > BD$ (als Seiten der Dreiecke AEB und BDA) und $y > x$ (als Winkel der Dreiecke BCE und ACD, deren Winkel bei C gleich und wo $\alpha > \beta$). Bringt man das Dreieck AEB in die Lage von BE_1A, wobei also $BE_1 = AE$, $q_1 = q$, $y_1 = y$, $b_0 = b_1 = a_1$, etc. und zieht die Gerade DE_1, so ist $n = m$ und $y_1 > x$, also $m + y_1 > n + x$, folglich $BD > BE_1$, oder $BD > AE$; was dem Vorigen, $AE > BD$, widerspricht; woraus man schliefst, dafs $\alpha_1 = \beta_1$ und somit das Dreieck ACB gleichschenklig sein mufs *).

Wenn dagegen beide Strahlen a_1, b_1 den Gegenseiten unterhalb der Grundlinie begegnen, wie in Fig. 4., so scheint der Beweis nicht auf analoge Weise Statt zu finden. Ich habe dafür den folgenden, minder einfachen aufgestellt.

Sollten α und β ungleich sein können, etwa $\alpha > \beta$, so wäre $BF > AF$ und daher $FD > FE$. Man nehme $FG = FA$ und $FH = FE$, so ist $GB = HD$ (weil nach der Voraussetzung $AD = BE$ oder $a_1 = b_1$). Ferner sind die Dreiecke HFG und EFA congruent, daher $\alpha_2 = \alpha_1 = \alpha$, mithin $\alpha_2 > \beta_1$, und folglich mufs die Gerade GH der Seite CB jenseit D, etwa in K begegnen, und zwar unter einem Winkel γ, welcher, wie leicht zu sehen, $= 2\varepsilon$ ist. Nun ist, vermöge des Dreiecks DAC, Winkel $\alpha_1 = C + D$, daher $\alpha > D$ (da $\alpha = \alpha_1$), und mithin $BD > BA$. Nimmt man $BL = BA$,

*) Man könnte übrigens auch wie folgt schliefsen. Wäre $\alpha_1 > \beta_1$, so wäre auch, wie oben, $y > x$ und $p > q$, und daher $AC > BC$; dagegen müfste, da die Dreiecke ACD und BCE, vermöge ihrer gleichen Winkel bei C und ihrer gleichen Seiten $AD = BC$, gleichen Kreisen eingeschrieben sind, und da $y > x$ ist, auch $BC > AC$ sein; was sich widerspricht: daher mufs $\alpha_1 = \beta_1$ und demzufolge $AC = BC$ sein. — Da dieser Beweis sich auf den Kreis stützt, so ist er nicht so elementar, wie der obige.

so sind die Dreiecke BAG und BLG congruent, also ist $\varepsilon_1 = \varepsilon$. Aber als äufserer Winkel des Dreiecks GLK ist $\varepsilon_1 > \gamma$, also auch $\varepsilon > \gamma$: was dem Vorigen, $\gamma = 2\varepsilon$, widerspricht: folglich können α und β nicht ungleich, d. h. das Dreieck ACB mufs gleichschenklig sein *).

Die obige Aufgabe (I.) kann übrigens auch etwas allgemeiner gestellt und doch eben so leicht gelöset werden, nämlich wie folgt.

Aufgabe II.

„Wenn die Winkel an der Grundlinie eines Dreiecks in gleichem Verhältnifs getheilt werden, so dafs $\alpha : \alpha_1 = \beta : \beta_1$, und wenn die bis an die Gegenseiten verlängerten Theilungslinien AD und BE gleich lang sind, so ist die Frage, ob dann das Dreieck gleichschenklig sei?"

Für die Fälle von (Fig. 1.) und (Fig. 3.) läfst sich auf ähnliche Weise, wie oben, zeigen, dafs das Dreieck auch unter den gegenwärtigen Bedingungen gleichschenklig sein mufs.

In Rücksicht des sphärischen Dreiecks lassen sich die beiden entsprechenden Aufgaben zum Theil auf fast gleiche Art elementar behandeln.

Aufgabe III.

„Wenn die beiden Hauptkreisbogen, welche die Winkel an der Grundlinie in einem sphärischen Dreieck hälften, von den Winkeln bis an die Gegenseiten genommen, gleich lang sind, so ist die Frage, ob dann das Dreieck gleichschenklig sei?"

Es sei im Dreieck ACB (Fig. 5.) Winkel $\alpha = \alpha_1$, $\beta = \beta_1$ und der Hauptkreisbogen $AD = BE$. Sollten α und β ungleich sein können, etwa $\alpha > \beta$, so wäre $BF > AF$, und daher $FD > FE$. Man nehme $FH = FA$ und $FG = FE$, so sind die Dreiecke AFE und HFG symmetrisch gleich, also Winkel $x_1 = x$ und $\alpha_2 = \alpha_1$. Da das Dreieck BFD offenbar grösseren Inhalt hat als das Dreieck HFG, so mufs auch seine Winkelsumme gröfser sein, als die des letztern: den Winkel bei F haben sie gemein, und von den übrigen ist $\alpha_2 > \beta_1$ (weil $\alpha_2 = \alpha_1 > \beta_1$), daher mufs Winkel $y > x_1$ und somit auch $y > x$ sein. Da ferner die Dreiecke BAD und ABE zwei Paar gleiche Seiten und dazwischen die ungleichen Winkel $\alpha > \beta$ haben, so ist Seite $d > e$ (d. i. $BD > AE$). Man denke sich nun das Dreieck ABE in der Lage von BAE_1, wo nämlich Winkel $x_2 = x$, $\gamma = \alpha + \alpha_1$. Seite

---

*) Auf fast ähnliche Art läfst sich auch der obige Fall (I.) beweisen.

$e_1 = e$ ($BE_1 = AE$), etc. ist, so wird man — falls der Winkel $DBE_1 = \gamma + \beta + \beta_1 < \pi$, d. h. falls die Summe der Winkel an der Grundlinie AB im gegebenen Dreieck ACB kleiner als zwei Rechte ist — durch Hülfe des Hauptkreisbogens DE_1, auf ganz gleiche Weise wie oben bei Fig. 2., auf den Widerspruch geführt, dafs $e_1 > d$, also $e > d$ sein müfste; woraus sodann auf die Gleichheit von α und β, und daraus auf die Gleichheit von AC und BC geschlossen wird.

Für die andere, allgemeinere Aufgabe, wo die Winkel an der Grundlinie, statt gehälftet, in irgend einem gleichen Verhältnifs getheilt werden, folgt auf gleiche Weise, dafs das Dreieck gleichschenklig sein mufs, falls die Summe der beiden Winkel an der Grundlinie kleiner als zwei Rechte ist.

Wenn dagegen die Summe der Winkel an der Grundlinie gröfser als zwei Rechte ist, so wird der Beweis für beide Aufgaben unbrauchbar. — Ich begnüge mich mit dieser Andeutung und überlasse es den Liebhabern, die vollständige, aber möglichst elementare Lösung aufzufinden.

26.
Von den vielfachen Puncten einer krummen Fläche.

(Von dem Herrn Prof. *Umpfenbach* in Giefsen.)

1.

Die Gleichung einer krummen Fläche sei $F(x,y,z)=0$; x, y, z seien die Coordinaten irgend eines Punctes A; x', y', z' die Coordinaten eines andern Punctes A' derselben: so ist auch $F(x',y',z')=0$.

Man nehme A zum neuen Ursprung an; die Coordinaten von A' in Beziehung auf denselben seien t, u, v, so ist, in der Voraussetzung, dafs die neuen Axen den vorigen parallel sind, $x'=x+t$, $y'=y+u$, $z'=z+v$; es ist also $F(x+t, y+u, z+v)=0$. Man entwickele das erste Glied dieser Gleichung nach dem Taylorschen Lehrsatze und bemerke, dafs $F(x,y,z)=0$. Es sei $\frac{\partial F}{\partial x}=P$, $\frac{\partial F}{\partial y}=Q$, $\frac{\partial F}{\partial z}=R$. Man nehme t, u und v verschwindend klein an, so ergiebt sich $Pt+Qu+Rv=0$. Dies ist die Gleichung einer Ebene, welche unendlich nahe bei dem neuen Ursprunge mit der krummen Fläche zusammenfällt, d. h. es ist die Gleichung der berührenden Ebene an dieser Stelle.

2.

Wenn nun die ursprünglichen Coordinaten von A so beschaffen sind, dafs sich durch deren Substitution P, Q und R in Null verwandeln, so verschwinden in der Entwicklung die Theilsätze, welche in Beziehung auf t, u und v von der ersten Dimension sind, und es bleiben, wieder unter der Voraussetzung, dafs A' unendlich nahe bei A liegt, nur die Theilsätze stehen, welche in Beziehung auf t, u und v von der zweiten Dimension sind. Setzt man nun $\frac{\partial P}{\partial x}=p$, $\frac{\partial P}{\partial y}=\frac{\partial Q}{\partial x}=l$, $\frac{\partial Q}{\partial y}=q$, $\frac{\partial P}{\partial z}=\frac{\partial R}{\partial x}=m$, $\frac{\partial Q}{\partial z}=\frac{\partial R}{\partial y}=n$, $\frac{\partial R}{\partial z}=r$, so erhält man für sämmtliche Puncte der krummen Fläche, welche unendlich nahe bei A liegen, die Gleichung:

$$(a.)\quad pt^2+qu^2+rv^2+2ltu+2mtv+2nuv=0;$$

in Beziehung auf welche die vier folgenden Fälle zu unterscheiden sind.

1) Wenn sich das erste Glied der Gleichung in das Product zweier ungleichen rationalen Factoren vom ersten Grade in Bezug auf t, u und v auflösen läfst, so kann jeder dieser Factoren für sich $=0$ gesetzt werden; durch A gehen also dann zwei Äste der krummen Fläche, deren jeder seine besondre berührende Ebene hat.
2) Wenn die beiden Factoren gleich sind, so fallen die beiden berührenden Ebenen in eine einzige zusammen.
3) Stellt die Gleichung ($a.$) ein imaginäres Verhalten zwischen t, u und v auf, so ist der Punct A ein isolirter conjugirter Punct der krummen Fläche.
4) Wenn keiner der drei Fälle Statt findet, so ist die Gleichung die einer krummen Fläche von der zweiten Ordnung, welche bei A mit der ursprünglichen krummen Fläche übereinstimmt.

Um also zu sehen, ob einer der Umstände in einem Puncte einer krummen Fläche, deren Gleichung gegeben ist, eintrete, setze man $\frac{\partial F}{\partial x}=P=0$, $\frac{\partial F}{\partial y}=Q=0$, $\frac{\partial F}{\partial z}=R=0$. Ergeben sich hieraus Werthe, welche der Gleichung der krummen Fläche ein Genüge leisten, so substituire man dieselben in die Gleichung ($a.$), und sehe dann, welcher der so eben bemerkten 4 Fälle eintritt.

Wenn jedoch durch die Substitution die Coëfficienten auch in dieser Gleichung Null werden, so bleibt in der Entwicklung die Summe der Theilsätze bestehen, welche in Beziehung auf t, u und v von der dritten Dimension sind, und die Untersuchung wird auf die nämliche Weise fortgesetzt.

Es wird hierbei vorausgesetzt, dafs in der Gleichung $F(x,y,z)=0$ die Nenner weggeschafft sind.

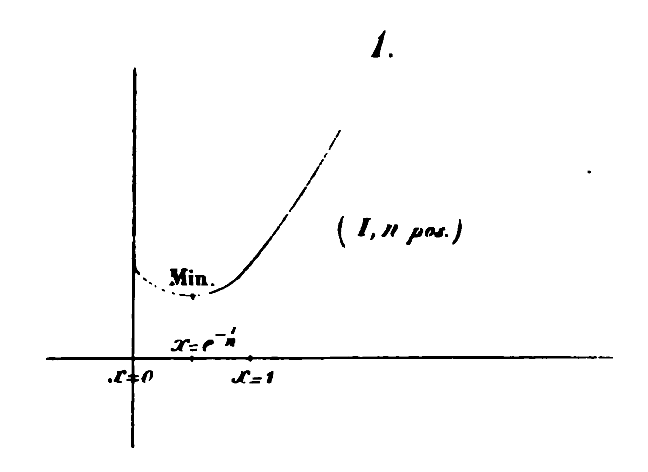
TAF. I.

Von

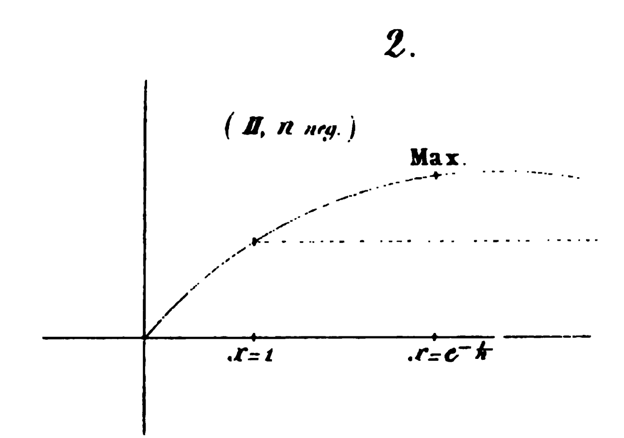
Die Gleichu
irgend eines
ben: so ist
Man
auf denselbe
gen parallel
Man entwic
bemerke, d
und v vers
chung eine
Fläche zus

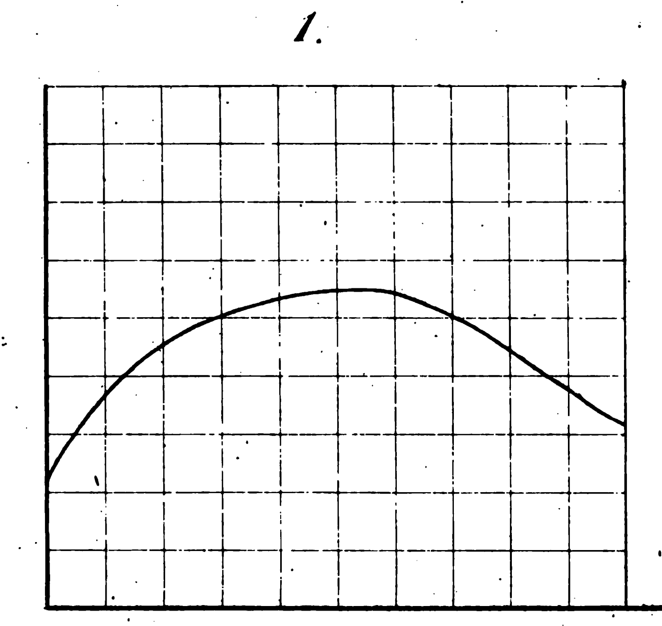
Wer
durch dere
Entwicklun
mension si
bei A liegt
zweiten Di
$\frac{\partial Q}{\partial z} = \frac{\partial R}{\partial y}$
welche un
in Beziehu
1) Wen
tiona
kann
zwei
2) Wen
in e
3) Stell
ist
4) Wer
Fläc
mer
Ur
Fläche,
$\frac{\partial F}{\partial z} = R =$
ein Genü
welcher
W
Null wer
in Bezieh
wird auf
E
weggesc

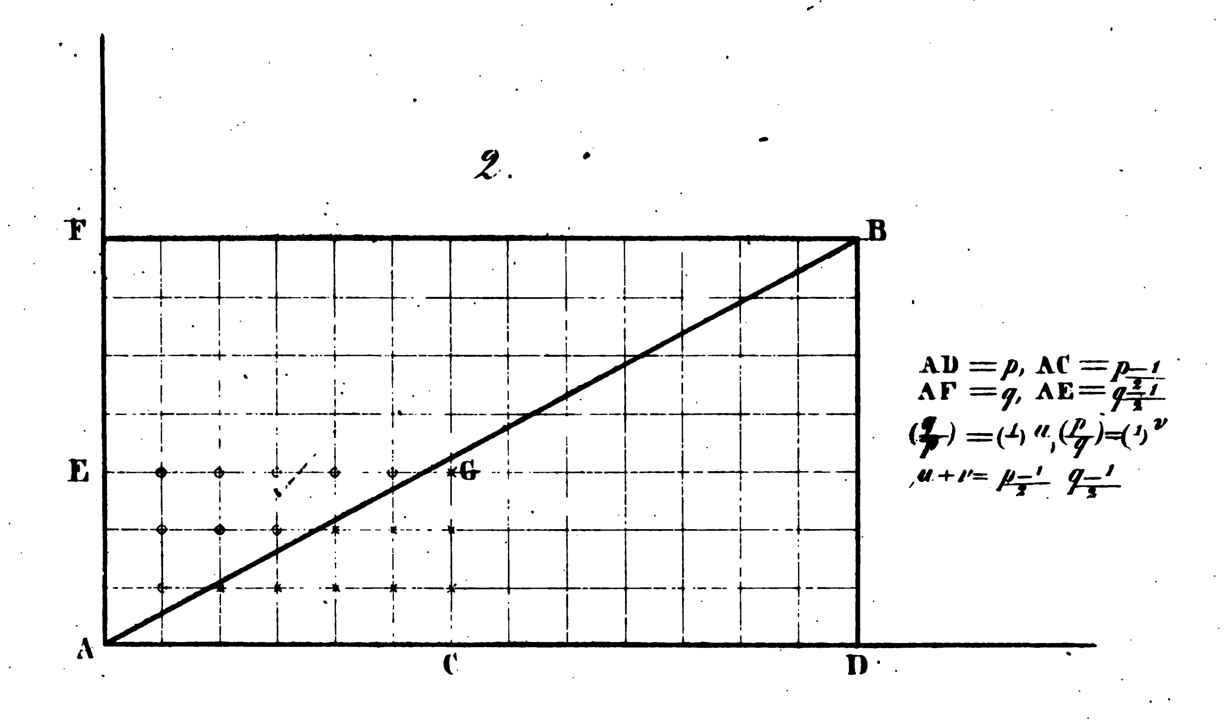
1.

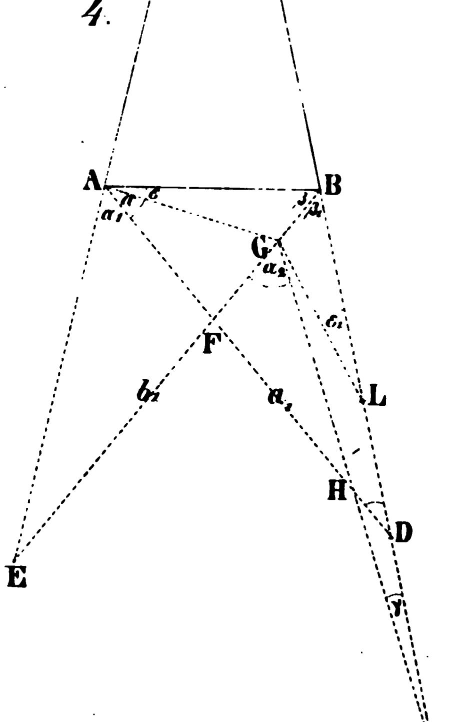


2.




1.


2.
F
B
E
G
A
C
D
AD = p, AC = (p−1)/2
AF = q, AE = (q−1)/2
(q/p) = (1)u, (p/q) = (1)v
u + v = (p−1)/2 · (q−1)/2


4.
C
A
B
G
F
L
H
D
E
K

STORAGE A

